CITADEL™

SECURITY SOFTWARE

CITADEL Hercules® Enterprise Vulnerability Management

Installation Guide

Citadel™ Security Software Inc.

Hercules® Installation Guide

Document Number: 204-01-0004

Hercules v4.0, Service Pack 2

Document Version: 1.2

November 2005

Acknowledgements

Citadel Security Software Inc. * Two Lincoln Centre * 5420 LBJ Freeway, Suite 1600 * Dallas, TX 75240
Phone: (214) 520-9292 * Fax: (214) 520-9293 * Email: support@citadel.com * Website: http://www.citadel.com

Contents

Glossary

Before You Begin

This section addresses the following topics:

- "About This Manual" describes the purpose, audience, and organization of this document as well as conventions used throughout all Hercules documentation.
- "Documentation Overview" describes the Hercules documentation distributed as PDF files and the context-sensitive online help.
- "Customer Support" contains contact information for Hercules technical support.
- "What's New?" describes the new features in the Hercules v4.0 Service Packs.

About This Manual

This section describes the purpose of the document, who it is written for, and how it is organized. It also lists the typographical conventions and reader alerts used in this manual. Additionally, it provides assistance in using the PDF file of this manual.

Purpose

The *Hercules Installation Guide* provides a guide through the entire process of installing the Hercules® software from planning, meeting requirements, and installing the software for the first time, to tasks you perform immediately after the initial installation.

Audience

This document is written to the Hercules administrator who is responsible for installing or upgrading the Hercules Server, Hercules Channel Server, and Hercules Download Server, and performing the initial setup on the Hercules Administrator after the installation.

Organization

This document is organized into the following chapters and appendixes. The document also contains a references section, a glossary, and an index.

“Preparing to Install”	Addresses planning considerations, provides a pre-installation checklist, and describes the minimum requirements for Hercules Servers, the Hercules Administrator, and Hercules Clients for each supported OS. It also addresses how to set up an SQL server for Hercules databases, SQL Report Services for Hercules reporting, and SQL server domain account configuration for enterprise reporting.
“Installing Servers and Administrator”	Describes installation scenarios, and gives step-by-step instructions for completing the Installation wizard to install the Hercules Servers and the Hercules Administrator for standalone and distributed architectures.
“Completing Post Installation Setup”	Provides instructions for setting up the software before handing it off to other administrators for configuration.
“Registration and Licensing”	Provides instructions on using a trial license and obtaining a retail license with licensed features.
“Migrating from a Previous Version”	Describes how to use the Hercules Data Migrator to migrate data from version 3.5.1, 3.5.1 SP1, or 3.5.1 SP2 to version 4.0 Service Pack 2.
“Removing Software Permanently”	Describes how to uninstall the product and delete all data.
“References”	Provides links to referenced third-party websites.
“Glossary”	Contains a glossary of terms used throughout this manual.

Typographical Conventions

This document uses these typographical conventions

Bold	Boldface text is used to highlight important names or information and to indicate options users select.
`Mono`	Mono-spaced text is used for actual code, command line input, file names, path names, and URLs.
`Bold Mono`	Boldface mono-spaced text identifies text users must type in the GUI
Italic	Document titles and for emphasis.
[ ]	Brackets enclose optional items in format and syntax descriptions.
< >	Angle brackets enclose variables in format and syntax descriptions.
{ }	Braces enclose a list from which you must choose a single item in format and syntax descriptions.
|	A vertical bar separates items in a list of choices in format and syntax descriptions.
…	An ellipsis in a syntax description indicates that the preceding item or line can be repeated one or more times. Otherwise, it indicates omitted information.

Reader Alerts

Citadel uses these reader alerts throughout its documents to notify you of supplementary and essential information.

Note - Alerts you to supplementary information.

Tip - Alerts you to information that can save you time, but is not essential to the task.

Important - Alerts you to information that is essential to completing the task.

Caution - Alerts you to possible data loss, requirement to repeat work, breaches of security, or other serious problems.

Warning - Alerts you that failure to take or avoid a specific action may result in physical harm to you or the hardware running Citadel Security Software.

Documentation Overview

Hercules software documentation includes Acrobat® PDF files and online help. This section describes the online help and the PDF documents that introduce you to Hercules software, help you install it, guide you in using it, and assist you with Windows lockdown issues.

PDF Files

The Hercules software includes PDF documents, that a user can display from the Hercules Administrator **Help** menu. These documents are also stored in the Hercules Administrator installation directory which is typically:

```
C:\Program Files\Citadel\Hercules\Administrator\Help
```

Additionally, you can access the *Hercules Security Configuration Guide* from the Hercules Security Portal on the navigation bar of the Hercules Administrator.

Introduction

- *Vulnerability Assessment and Remediation Overview* (`VulGuide.PDF`)—Introduces the best practice workflow of device discovery, vulnerability assessment, vulnerability review, vulnerability remediation, and vulnerability management, where the device discovery and vulnerability assessment processes assume the existence of scans, generated by third-party tools, that can be imported by the Hercules Administrator.
- *Hercules Quick Start Guide* (`QuickStart.PDF`)—Guides the new user through one path of the Hercules QuickStart Remediation wizard. With this guide, you discover and select devices for QuickStart remediation through Active Directory, select a predefined policy that identifies vulnerabilities, enforce that policy, and produce a report from the automated vulnerability remediation.

Installation

- *Hercules Installation Guide* (`InstallGuide.PDF`)—Contains instructions on preparing for the installation, installing and registering the Hercules software, completing post-installation setup tasks, and migrating from a previous version.
- *Creating Network Install Package for Microsoft Internet Explorer 6.0* (`IEAK.PDF`)—Provides instructions on setting up the installation package that is required for using Hercules functionality to remediate vulnerabilities on Microsoft Internet Explorer 6.0.
- *Using Hercules and Administrative Network Installation Points to Remediate Microsoft® Office 2000* (`Office2000.PDF`)– Provides instructions for setting up the installation package that is required for using Hercules functionality to apply service packs to Microsoft Office 2000 systems.

Operations and Maintenance

- *Hercules User's Guide* (`UserGuide.PDF`)—Provides a product overview, procedures for configuring and using the Hercules system as well as a reference section that describes each window in the Hercules administrator console.
- *Hercules Remedy Actions Reference* (`HercRemedyGuide.PDF`)—Describes actions for building custom remedies, including properties and values.
- *Hercules Reporting Schema* (`HerculesReportingSchema.PDF`)—Describes the Hercules Server and inventory database views that the Hercules Server Reporting feature and the Enterprise Reporting feature access and use to generate reports.

Windows Lockdown

- *Hercules Security Configuration Guide*—Contains recommendations for progressively locking down the Windows Server 2003™ and Windows 2000 Server machines on which the Hercules Servers, Hercules Channel Server, and Hercules Download Server are installed. (This post-release document is available from the Hercules Security Portal on the navigation bar of the Hercules Administrator.)

Online Help

The Hercules Administrator online help provides a context-sensitive reference for some of the Hercules system web pages and dialog boxes, including descriptions of data entry fields and allowed values. When you click the Help button or press F1 in any window or dialog box of the Hercules Administrator, the system displays a context-sensitive topic. Within a topic, you can click the links to navigate to other topics.

Customer Support

When you purchase a Customer Support Agreement and register your Citadel software product, you are eligible to receive technical support according to the terms of the contract you purchased. Citadel provides two levels of technical support:

- **Standard support**—Available by phone 7 A.M. - 7 P.M. US Central Standard Time on normal Citadel Security Software business days.
- **Premium support**—Available by telephone, 24 hours x 7 days x 365 days of the year.

Registered users can reach Citadel Customer Support using the:

- Toll-free hot line at 888-9-CITADEL (888-924-8233)
- E-mail address at `support@citadel.com`
- Customer Support Portal on the Internet site at `http://www.citadel.com/`

What's New?

Hercules v4.0, Service Pack 2

Service Pack 2 provides the following new installation functionality:

- New Local Groups include *HerculesChannelServerUsers* and *HerculesDownloadServerUsers*. During installation, the installer's Windows identifier is added to each of these new local groups. The installer and any Windows users or groups manually added to these Local Groups are given access to the Hercules Channel Server web site and the Hercules Download Server web site, respectively. See the post-installation procedure, "Grant User Access to the Channel Server and Download Server" (page 3-2).
- The installation for SP2 modifies the Channel Server ASPs and Download Server ASPs to require windows authentication. Therefore, the procedure on how to prevent anonymous access to these Active Server Pages has been removed from the chapter on Completing Post-Installation Setup.
- The licensing process has changed. Changes are reflected in "Registration and Licensing" (page 4-1).
- The upgraded Data Migration Tool allows migration of existing 3.5.1 data to 4.0.x. The chapter, "Migrating from a Previous Version" (page 5-1) has been significantly enhanced and now includes tips from Citadel Customer Support.

Hercules v4.0, Service Pack 1

Service Pack 1 adds Hercules Client support for Mac OS X versions 10.2, 10.3, and 10.4. See "Hercules Client for Mac OS X Requirements" (page 1-16).

1. Preparing to Install

Pre-installation planning makes it possible to optimally configure the Hercules enterprise security software with the first installation and ensures scalability when additional clients are considered for remediation. This section provides guidelines to help you with this process. Citadel will help you plan the best configuration for your system; contact Customer Support for assistance.

This section addresses the following topics:

Note: If you are upgrading from v3.5.1, you may benefit from reviewing migration approaches as part of your planning. See "Migration Approaches" on page 5-1.

Planning Considerations

Planning involves making decisions in the following areas:

Site Selection

The Hercules Server is an integral component of network security, and you should install it where production servers are located. Installing the Hercules Server in a controlled environment such as a data center or server room provides greater stability and security. For more details on controlled environments, see *Hercules Security Configuration Guide.*

Architecture

Hercules software includes three types of servers:

- Hercules main server
- Hercules Channel server
- Hercules Download server

You can install these three components on the same physical Windows server in a standalone configuration or across multiple servers in a distributed configuration. The Hercules Server is the core server. The Channel Server helps communication between the Hercules Server and the Hercules Download Server. The Hercules Download Server downloads files from Internet sites on.

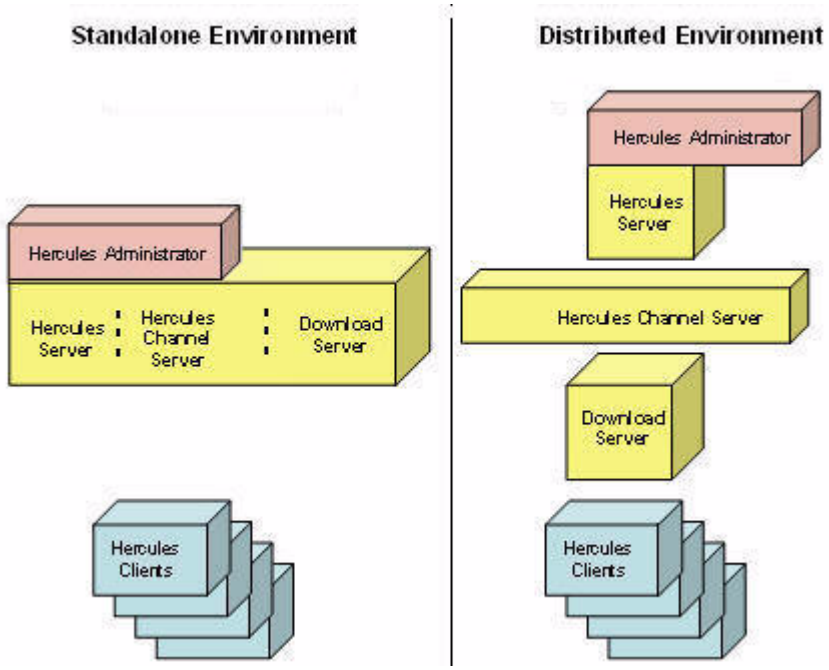


Figure 1-1. Standalone and Distributed Environment Differences

Distribution of Licenses

A Hercules Server can service approximately 2,000 licenses, one for each device where a Hercules client is installed. Contact Citadel for licensing recommendations beyond this number. You can easily add new licenses to a server, unless you have exceeded the maximum number of licenses that can be supported by the server. However, you cannot easily redistribute licenses once they are assigned. To remove a license from the Hercules Server, you must un-install and reinstall the Hercules Server. To avoid this situation, estimate carefully how to distribute the licenses to support future growth.

Server Hardware Selection Parameters

The Hercules software includes one or more server components that provide remediation services to Hercules Clients. When selecting the hardware platform on which to install Hercules, you should consider these factors:

- Number of devices to be remediated
- Frequency of remediation and remediation content
- Whether the Hercules Server is dedicated or shared by other applications

Depending on the number of clients and remediation content, multiple processor machines and additional memory can increase the number of simultaneous remediations that a Hercules Server can accommodate. Additional servers can also be added as additional clients are defined for remediation. This simplifies the scalability issue for the system administrator by simply adding a new server to handle the additional client load.

Bandwidth Considerations

The Hercules software uses minimal network bandwidth during the remediation process. However, if a remediation requires patch installation, the Hercules system must download the required patch from the Hercules Download Server to the Hercules Client and then perform the installation. Since patches vary in size, the required bandwidth for remediation depends on the needs of each remediation. You should place the Hercules Download Server near the Hercules Clients to take advantage of LAN bandwidth. Citadel recommends that you create small groups of Hercules Clients and stagger their remediation schedules. This precaution prevents all clients from performing remediations simultaneously. Multiple servers can also accommodate bandwidth issues by distributing the workload.

Security and Permission Requirements

The administrator who installs Hercules must also have access to the SQL database. That is, this user must be the administrator of the local machine and and have administrative access to the SQL Server and its SQL Server instance. The credentials used to access the SQL database must be the same credentials used when logging on to install the Hercules system.

Local or Remote SQL Server

A Hercules installation requires the following:

- Hercules v4.0 main server
- SQL server
- Reporting Services

With either standalone or distributed configuration, you can install the Hercules main server on the same machine with the SQL server and/or Reporting Services or on a separate machine.

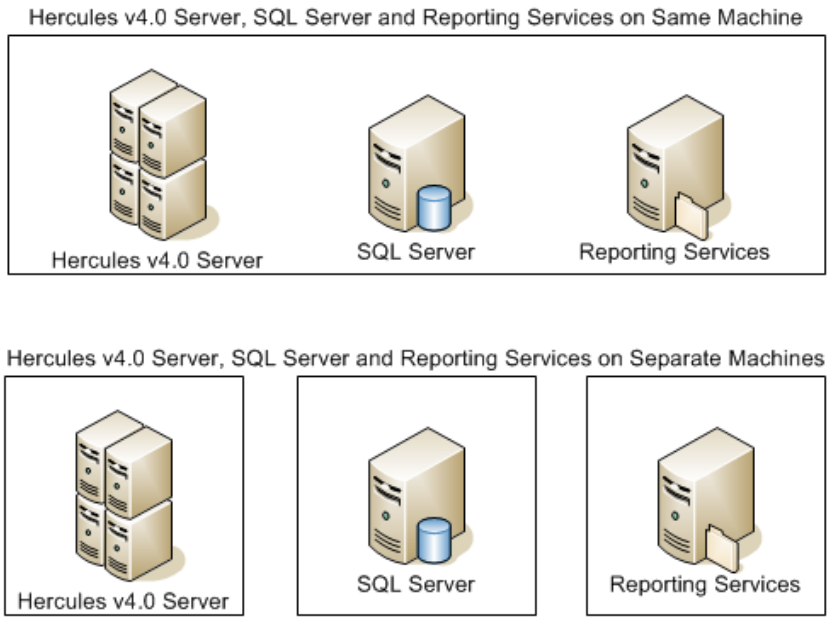


Figure 1-2. Installation Options for Hercules Server, SQL Server, and Reporting Services

Database Requirements and Usage

A Microsoft® SQL Server™ 2000 Service Pack 3a must be available for use to the physical machine where the Hercules Server is to be installed. If installing the Hercules Server on a machine with an SQL Server 2000 and that server is below the required patch level, you must update this server to SP3a before installing the Hercules Server. Multiple Hercules Servers can use the same SQL server. If you install the Hercules Channel Server or Hercules Download Server on a different machine from the one where you install the Hercules Server, the installation process installs MSDE 2000 Service Pack 3a as part of the Hercules Channel Server and the Hercules Download Server installation. This instance of MSDE 2000 is of the type that can be patched.

Important - The Hercules databases are stored where the master database for the SQL server resides. Specifically, the installation process installs the Hercules Server's database files (`Hercules.ldf` and `Hercules.mdf`) in the same directory as the SQL Server's Master database files (`master.ldf` and `master.mdf`.).

SQL Reporting Server Selection

Identify a server with SQL reporting web services to use for Hercules Reporting. SQL Reporting Services SP1 is required with an additional KB of disk space. You may install the Hercules server on a machine where SQL reporting web services runs locally. See "Install SQL Server 2000 and SQL Server 2000 Reporting Services" (page 1-17). If you plan to install multiple Hercules Servers, your IT manager may want them all to use the same server for Hercules reporting. The SQL Reporting Server URL is specified during the Hercules Server installation process.

The SQLService must be running as a user that can authenticate to the Hercules Server (either via domain auth or pass-thru). Create a user on the server with the main Hercules server. This user does not have to be an administrator. See "Configure Enterprise Reporting" on page 1-22.

Migration Considerations

If you have been using Hercules v3.5.1, keep it operational while you install Hercules v4.0. After Hercules v4.0 is running, you can run the Hercules Migration Tool to move your Hercules data to the Hercules v4.0 databases. You can migrate from one active database to the other if the two software versions are on separate machines. For in-place migration, you can use a backup file.

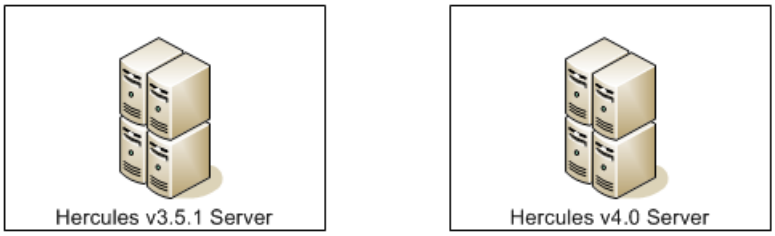


Figure 1-3. Keep v3.5.1 and v4.0 Hercules Servers Running in Parallel Until Data Migration

Pre-Installation Checklist

Before installing the Hercules software, ensure these prerequisites are met:

- You are an administrator on the machine(s) where you plan to install the Hercules servers (Hercules Server, Hercules Download Server, Hercules Channel Server).
- You have Administrator privileges on the SQL Server machine and its SQL Server instance, if installing Hercules with a remote SQL Server.
- The SQL Server runs as a user that the Hercules Server's machine can authenticate using domain authentication or pass-through.
- If the SQL Server is in a workgroup, the Hercules Server must be in that same workgroup.
- All hardware and software meet the requirements listed in
  - — "Server Installation Minimum Requirements" (page 1-7)
  - — "Hercules Administrator Installation Minimum Requirements" (page 1-11).
  - — "Hercules Client Installation Minimum Requirements" (page 1-12)
- Required Windows components are installed.
  - — Microsoft IIS, Microsoft ASP.NET, and ASPs. See "Verify or Install Required Windows Components" (page 1-8).
  - — Microsoft .NET v1.1 Framework. If missing, load it from your Hercules CD or directly from the Microsoft Windows Updates. See "Download Microsoft NET v1.1 Framework" (page R-1).
  - — Internet Explorer 6 with Service Pack 1.
- SQL Server 2000 SP3a and SQL Server 2000 Reporting Services SP1 are installed. See "Install SQL Server 2000 and SQL Server 2000 Reporting Services" (page 1-17).
- A Hercules User Group must exist on the machine where Reporting Services is installed. Add Windows credentials for users who will be accessing Hercules Reports. See "Populate Hercules User Group on Reporting Machine" (page 1-21).
- For Enterprise Reporting, see "Configure Enterprise Reporting" (page 1-22).

Server Installation Minimum Requirements

This section provides tables of information that will enable you to:

Verify Software Requirements

Hercules Server Software Requirements

The Hercules Server, Hercules Channel Server, and Hercules Download Server can all be installed on the same machine. The SQL Server and SQL Reporting Services can each be installed on the machine with the Hercules Server or on a different machine.

Type	Hercules Server Components	Comments
Operating Systems	Windows 2000 Server, Service Pack 4 (SP4) Windows 2000 Advanced Server, SP4 Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition	• The Hercules Server cannot be installed on a machine that is a Primary Domain Controller (PDC), a Backup Domain Controller (BDC), or an Active Directory Controller (ADC). • Software, IIS and Web Browser must be installed prior to installing the Hercules Server.
Processor	Pentium® 4, 2 GHz or above	
Network Interface	100 Mb/s	
Free Disk Space	2.8 GB for server installation (Allow an additional 7 mb/device if licensing AssetGuard.) Hercules Download Server: 2.8 GB + 10-20 GB for file downloads	
VGA Graphics	1024x768 resolution	
Web Browser	Internet Explorer® 6.0	
Web Server	IIS 5.0 (Windows 2000 Server family) IIS 6.0 (Windows Server 2003 family)	
Software	Microsoft SQL Server 2000 SP3a Microsoft Reporting Services SP1 Microsoft.NET Framework v1.1 Microsoft ASP.NET Microsoft Internet Information Server (IIS) Adobe Acrobat Reader™ 5.0 or higher	If running the Hercules server on Windows Server 2003, enable IIS and ASP.NET 1.1. (They are disabled by default.) For details on SQL Server 2000 and Reporting Services, see "SQL Server and Reporting Services Setup" on page 1-17.

Hercules Channel Server Software Requirements

The Hercules Channel Server has the same requirements as the Hercules Server.

Hercules Download Server Software Requirements

The Hercules Download Server has the same requirements as the Hercules Server, except the Download Server requires an additional 10-20 GB of disk storage space for file downloads.

Verify Memory Requirements

The maximum number of devices that the Hercules system can support depends on the amount of Random Access Memory (RAM) installed in the machines on which the Hercules Server and the Hercules Administrator are installed. This table lists the recommended RAM amounts.

Number of Devices (Clients)	Hercules Server Memory Requirements	Hercules Administrator Memory Requirements
500	1 GB	256 MB
1000	1.5 GB	512 MB
2000	2 GB	512 MB

Verify or Install Required Windows Components

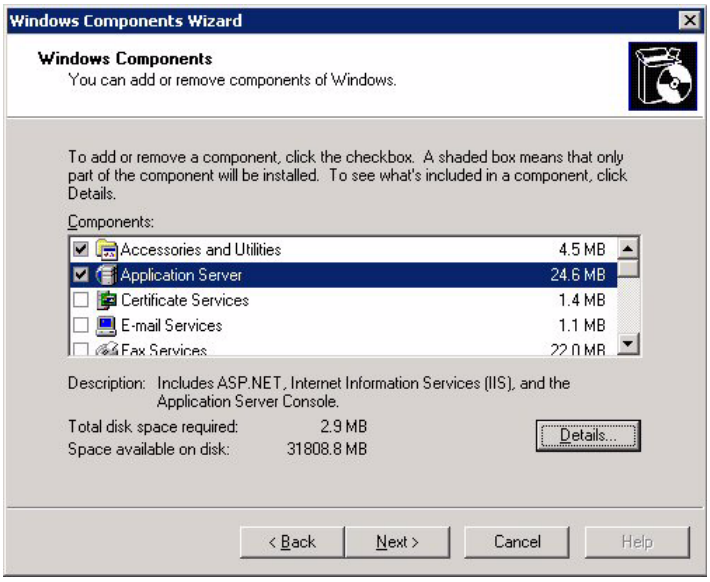
These Windows components must be installed on the machine where you install the Hercules Server:

- Internet Information Services (IIS)
- ASP.NET
- Active Server Pages (ASP)

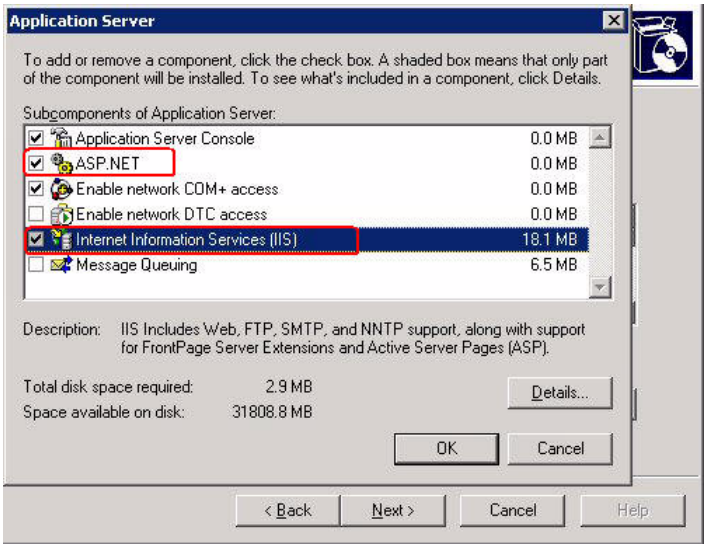
Note: These guidelines are for Windows Server 2003, but the process is similar for a Windows 2000 Server. (Windows 2000 Server requires IIS 5.0 or higher.)

To add the required Windows Components

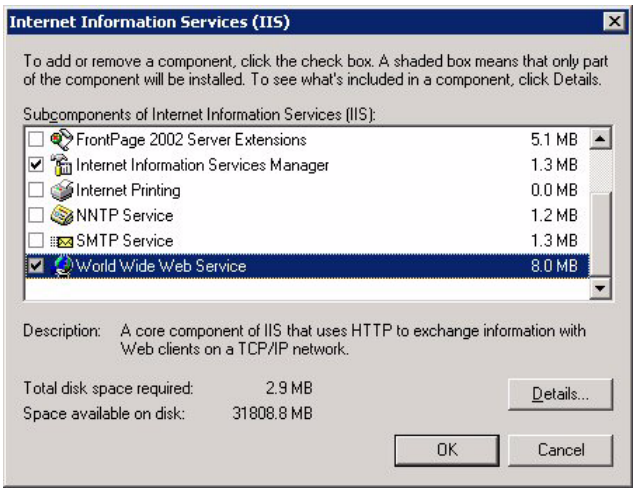
1. From the Control Panel, select **Add or Remove Programs**.
2. Click the **Add/Remove Windows Components** button on the tool bar to open the Windows Components Wizard.



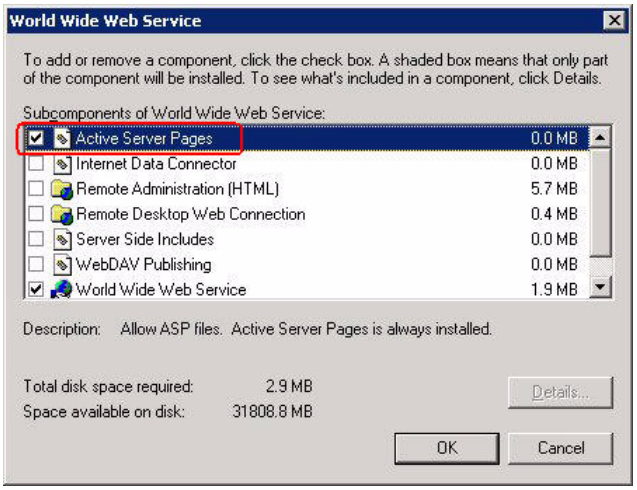
3. Select **Application Server** and click **Details** to open Application Server. Verify the following two items are checked: **ASP.NET** and **Internet Information Services (IIS)**



4. Select **Internet Information Services (IIS)** and click **Details** to open Internet Information Services (IIS).



5. Scroll to **World Wide Web Service**, select it, and click **Details** to open World Wide Web Service.



6. Click the check box to add the **Active Server Pages** component.
7. Click **OK** to exit World Wide Web Service.
8. Click **OK** to exit Internet Information Services (IIS).
9. Click **OK** to exit Application Server.
10. From the Windows Components Wizard, click **Next** to make the configuration changes you requested.
11. Click **Finish** to exit the wizard.

Hercules Administrator Installation Minimum Requirements

The maximum number of devices that the Hercules system can support depends on the amount of Random Access Memory (RAM) installed in the machines on which the Hercules Server and the Hercules Administrator are installed. This table lists the recommended RAM amounts.

Number of Devices (Clients)	Memory Requirements
500	256 MB
1000	512 MB
2000	512 MB

The following table describes other minimum requirements for the Hercules Administrator.

Type	Hercules Administrator Components	Comments
Operating Systems	Windows 2000 Server, SP4 Windows 2000 Advanced Server, SP4 Windows 2000 Professional, SP4 Windows XP Professional Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition	• The Hercules Administrator can run on the same machine as the Hercules Server, but additional disk space and memory is required. • The user of the Hercules Administrator must have either a valid local Microsoft Windows account on the Hercules Server or a domain account that the Hercules Server recognizes. • The .NET Framework version 1.1 is a component of the Microsoft Windows® operating system used to build and run Windows-based applications. You can download this from the Hercules Components page when you download the Hercules Administrator. Or, you can download it in advance from Microsoft. See “Download Microsoft NET v1.1 Framework” (page R-1).
Processor	Pentium III, 750 MHz or above	
Memory	See above	
Free Disk Space	1 GB or above	
VGA Graphics	1024x768 resolution	
Network Interface	100 Mb/s	
Web Browser	Internet Explorer 5.5 or above	
Software	Microsoft .NET Framework v1.1 Adobe Acrobat Reader 5.0 or higher See “Download Adobe Reader” (page R-1) Windows 2000 High Encryption Pack (required when installing the Administrator on Windows 2000.) See “Download Windows 2000 High Encryption Pack” (page R-1).	

Hercules Client Installation Minimum Requirements

For each of the Hercules clients, there is a minimum set of installation requirements:

- "Hercules Client for Microsoft Windows Requirements"
- "Hercules Client for Solaris Requirements"
- "Hercules Client for Linux Red Hat Requirements"
- "Hercules Client for AIX Requirements"
- "Hercules Client for HP-UX Requirements"
- "Hercules Client for Tru64 Requirements"
- "Hercules Client for Mac OS X Requirements"

Hercules Client for Microsoft Windows Requirements

Type	Components for Hercules Client for Microsoft Windows	Comments
Operating Systems	Windows NT® 4.0 Workstation, SP6 Windows NT® 4.0 Standard Server, SP6 Windows NT® 4.0 Terminal Server, SP6 Windows 2000 Server Windows 2000 Advanced Server Windows 2000 Professional Windows XP Professional Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition	• Disk space for patch downloads depends on size of patches, service packs, and hot fixes.
Processor	Pentium	
Memory	64 MB RAM	
Free Disk Space	15 MB for client installation 5 GB for patch downloads 1 GB for the initial rollback snapshot, if rollback is enabled	
Web Browser	Internet Explorer 5.5 SP2, only for 'Windows NT 4.0 platforms	
Security	SSL used for secure communications	

Hercules Client for Solaris Requirements

Type	Solaris Components	Comments
Operating Systems	Solaris™ 2.6, 7, 8, 9, 10	• Hercules Client operates at run level 3 • Outbound access via HTTP/HTTPS • (SSH) Inbound root access via TCP/IP port 22 • Patch clusters recommended for downloads • Disk space for patch download depends on size of patches and packages to download. • Install gzip and unzip in /bin or /usr/local/bin so client can unzip Solaris packages.[a] • Citadel recommends sudo access for enhanced security.
Processor	SPARC®	
Memory	64 MB RAM	
Free Disk Space	15 MB in /opt for client installation and message logging 200 MB for patch downloads to `/opt/citadel/hercules/download`	
Software	(Solaris 2.6 only) gzip for `2.6_Recommended.tar.Z` files[a]	
Security Software	• OpenSSH v3.5p1 or higher • SSL/HTTPS enabled with OpenSSL 0.96 or higher • (Solaris 8 only) requires patch 112438-01 to enable SSL and SSH • Sudo v1.6.7 or later (for Sudo client CSM functionality)	

a.If you are running Solaris 2.6, and want to remediate a vulnerability that requires the `2.6_Recommended.tar.Z` file downloaded from `sunsolve.sun.com` and installed on the server, you must first have the `gzip` package installed. It does not come installed by default in Solaris 2.6. Solaris 7, 8, 9, and 10 do not have this issue.

Hercules Client for Linux Red Hat Requirements

Type	Red Hat Components	Comments
Operating Systems	• Red Hat Desktop 7.3, 8, 9 • Red Hat Enterprise Linux AS 2.1, 3.0, 4.0 • Red Hat Enterprise Linux ES 2.1, 3.0, 4.0 • Red Hat Enterprise Linux WS 2.1, 3.0, 4.0	• Hercules Client operates at run level 3 • Outbound access via HTTP/HTTPS • Disk space for patch downloads depends on size of RPMs to download.
Processor	Pentium class	
Memory	64 MB RAM or above	
Free Disk Space	15 MB in /opt for client install and msg logging 200 MB for patch downloads to /opt/citadel/hercules/download	
Security Software	• OpenSSH v3.5p1 or higher • SSL/HTTPS enabled with OpenSSL 0.9.6 or higher • Sudo v1.6.7 or later (for Sudo client CSM functionality)	• (SSH) Inbound root access via TCP/IP port 22. • Citadel recommends sudo access for enhanced security. By default, sudo is installed with Red Hat v8 and v9.

Hercules Client for AIX Requirements

Type	AIX Components	Comments
Platforms	AIX 5.1, 5.2, 5.3	• Hercules Client operates at run level 2. • Outbound access is via HTTP/HTTPS. • Disk space for patch downloads depends on size of bff or .tar.gz files to download.
Processor	PowerPC™	
Memory	128 MB RAM or above	
Free Disk Space	15 MB in /opt for client installation 2 GB for patch downloads in `/opt/citadel/hercules/download`	
Security Software	• OpenSSH v3.5p1 or higher • SSL/HTTPS enabled with OpenSSL 0.9.6 or higher • Sudo v1.6.7 or later (for Sudo client CSM functionality)	• (SSH) Inbound root access via TCP/IP port 22. • Citadel recommends sudo access for enhanced security.

Hercules Client for HP-UX Requirements

Type	HP-UX Component	Comments
Platforms	HP-UX 11.0, 11iv1	• Hercules Client operates at run level 3. • Outbound access via HTTP/HTTPS. • Disk space for patch downloads depends on size of the depot files to download.
Processor	PA-RISC™	
Memory	128 MB RAM or above	
Free Disk Space	15 MB in /opt for client install 1 GB for patch download in `/opt/citadel/hercules/download`	
Software	Requires the following or superseding patches: PHSS_28869 (for HP-UX 11.0) PHSS_28871 (for HP-UX 11i v1)	• "Download required patches from http://www.itrc.hp.com" (page R-1)
Security Software	• OpenSSH v3.5p1 or higher • SSL/HTTPS enabled with OpenSSL 0.9.6 or higher • Sudo v1.6.7 or later (for Sudo client CSM functionality)	• (SSH) Inbound root access via TCP/IP port 22. • Citadel recommends sudo access for enhanced security.

Hercules Client for Tru64 Requirements

Type	HP-UX Component	Comments
Platforms	Tru64 5.1B	• Hercules Client operates at run level 3. • Outbound access via HTTP/HTTPS. • Disk space for patch downloads depends on size of the depot files to download. • The Tru64 "Enhanced Security" mode is not supported.
Processor	"400"	
Memory	128 MB RAM or above	
Free Disk Space	15 MB in /opt for client install 1 GB for patch download in `/opt/citadel/hercules/download`	
Security Software	• OpenSSH v3.5p1 or higher • SSL/HTTPS enabled with OpenSSL 0.9.6 or higher • Sudo v1.6.7 or later (for Sudo client CSM functionality)	• Native SSH needs to be replaced with OpenSSH/OpenSSL if Hercules Client Management Services (CMS) is to be used to install Hercules Clients or to support uninstall, reboot, start, stop, remediate, and sudocheck.

Hercules Client for Mac OS X Requirements

Type	HP-UX Component	Comments
Platforms	Mac OS X 10.2, 10.3, and 10.4	• Hercules Client runs as a daemon. • Outbound access via HTTP/HTTPS. • Disk space for patch downloads depends on size of the disk image (dmg) to download.
Processor	PowerPC™	
Memory	128 MB RAM or above	
Free Disk Space	15 MB in /opt for client install 200 MB for patch download in `/opt/citadel/hercules/download`	
Security Software	• OpenSSH v3.6p1 or higher[a] • SSL/HTTPS enabled with OpenSSL 0.9.6 or higher • Sudo v1.6.7 or later (for Sudo client CSM functionality)	• SSH inbound root access via TCP/IP port 22. • Citadel recommends sudo access for enhanced security. By default, sudo is installed with the Mac OS X.

a.This version is different than that required for the other clients.

SQL Server and Reporting Services Setup

If installing the Hercules Server on a separate machine from the SQL Server machine, create an account called "HerculesAdministrator" and add it to the Administrator's group on both the SQL Server and Hercules Server machines. Its password must be the same on these two machines. In a domain, using the domain administrator's account to install Hercules is sufficient.

This section includes the following procedures required for Hercules Reporting.

- "Install SQL Server 2000 and SQL Server 2000 Reporting Services" (page 1-17). Installing the SQL Server 2000 is a minimum requirement for the Hercules Server.
- "Populate Hercules User Group on Reporting Machine" (page 1-21)
- "Configure Enterprise Reporting" (page 1-22)

Install SQL Server 2000 and SQL Server 2000 Reporting Services

This section includes:

- Procedure for installing Reporting Services on a "Windows 2000 Server, SP4" (page 1-17)
- Procedure for installing Reporting Services on a "Windows Server 2003" (page 1-19)

Windows 2000 Server, SP4

The following instructions assume you are installing SQL Server 2000 and SQL Server 2000 Reporting Services locally. Remote installations will require some adjustments. It is also assumed that SSL will not be used.

To install SQL Server on Windows 2000 Server

1. Install .NET 1.1 (if not already installed).
2. Install SQL Server 2000.
   - Use a trusted domain account for both services, that is, a user ID and password that can be shared on multiple machines. This will ease report replication deployment.
   - Select the **Autostart** checkbox for both services.
   - Use Windows authentication mode.
3. Install SQL Server 2000 SP3a.

To install Reporting Services on Windows 2000 Server

1. Install SQL Server 2000 Reporting Services.
   - The system prerequisites check may inform you that VS .NET 2003 is not installed. This is OK, so click **Next.**

- On the Service Account dialog box, use the default built-in account (NT AUTHORITY\SYSTEM).

- On the Reporting Services Virtual Directories dialog box, use the defaults except *uncheck* the **Use SSL** checkbox.

- On the Report Server Database dialog box, select `Domain User Account` from the **Credentials Type** dropdown. Then specify your local Administrator account. For example, `username=Adminstrator, password=<your password>, domain=<your machine name>`.
- Skip the Report Server Delivery Settings dialog.

Note: Notice whether the final dialog reports that **`Setup could not initialize the report server.`** How you complete Step 4 depends on this result.

2. Install SQL Server 2000 Reporting Services SP1
3. Install SQL Server 2000 Reporting Services documentation update (optional)
4. Do one of the following:
   - If the final dialog reports that **`Setup could not initialize the report server`**, enter the following from the command prompt:

     ```
     rsconfig -c -s <servername> -d ReportServer -a Windows -u
     <servername>\Administrator -p <password>
     ```

     ```
     rsactivate -c "C:\Program Files\Microsoft SQL
     Server\MSSQL\Reporting
     Services\ReportServer\RSReportServer.config" -u
     <servername>\Administrator -p <password>
     ```

     ```
     c:\winnt\Microsoft.NET\Framework\v1.1.4322\aspnet_regiis -i
     ```

     ```
     iisreset
     ```

   - If the final dialog in Step 1 does not report a failure to initialize the report server, continue with the next step.
5. Restart the Report Server windows service.
6. From the **Start** menu, select **Programs > Microsoft SQL Server > Reporting Services > Report Manager**

Windows Server 2003

The following instructions assume you are installing SQL Server 2000 and SQL Server 2000 Reporting Services locally. Remote installations will require some adjustments. It is also assumed that SSL will not be used.

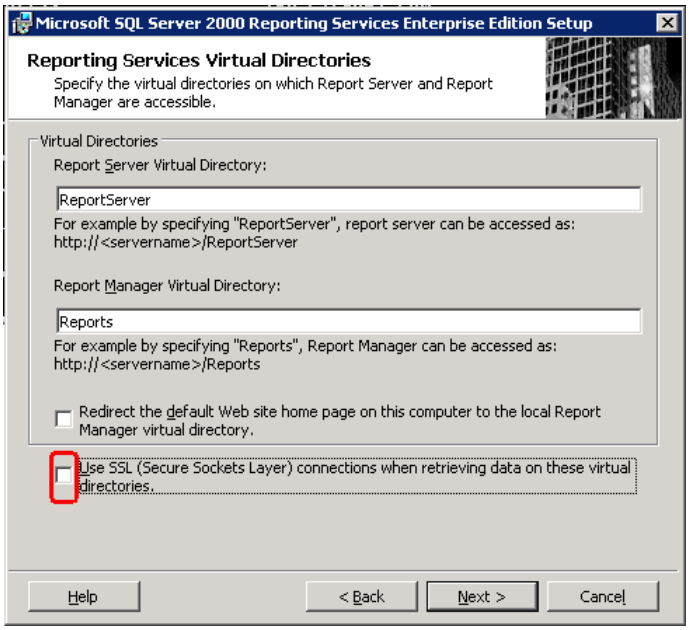
To install SQL Server 2000 on Windows Server 2003

1. Install SQL Server 2000.
   - Use a trusted domain account for both services (i.e. a user ID and password that can be shared on multiple machines). This will ease replication deployment if you plan on installing the Hercules server.
   - Select the **Autostart** checkbox for both services.
   - Use Windows authentication mode.
2. Install SQL Server 2000 SP3a.

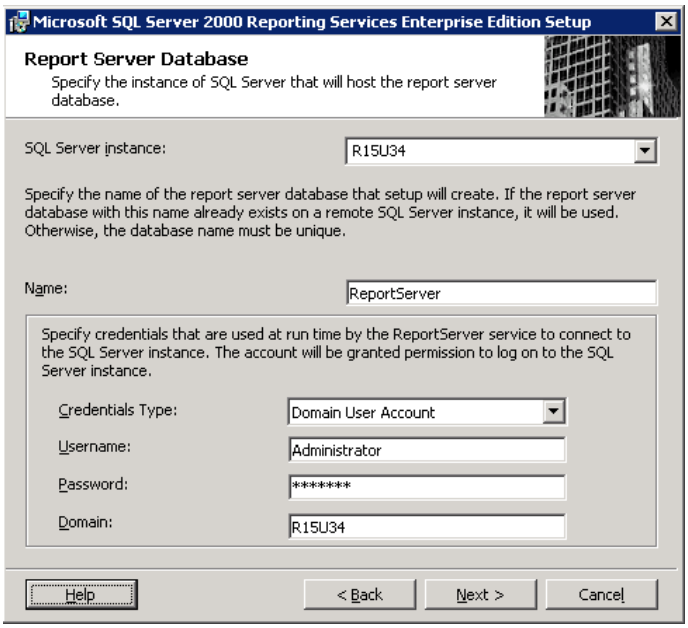
To install Reporting Services on Windows Server 2003

1. Install SQL Server 2000 Reporting Services.
   - The system prerequisites check may inform you that Visual Studio .NET 2003 is not installed. This is OK, so click **Next.**
   - On the Service Account dialog box, use the default built-in account (NT AUTHORITY\NETWORK SERVICE).

   - On the Reporting Services Virtual Directories dialog box, use the defaults except uncheck the **Use SSL** checkbox.



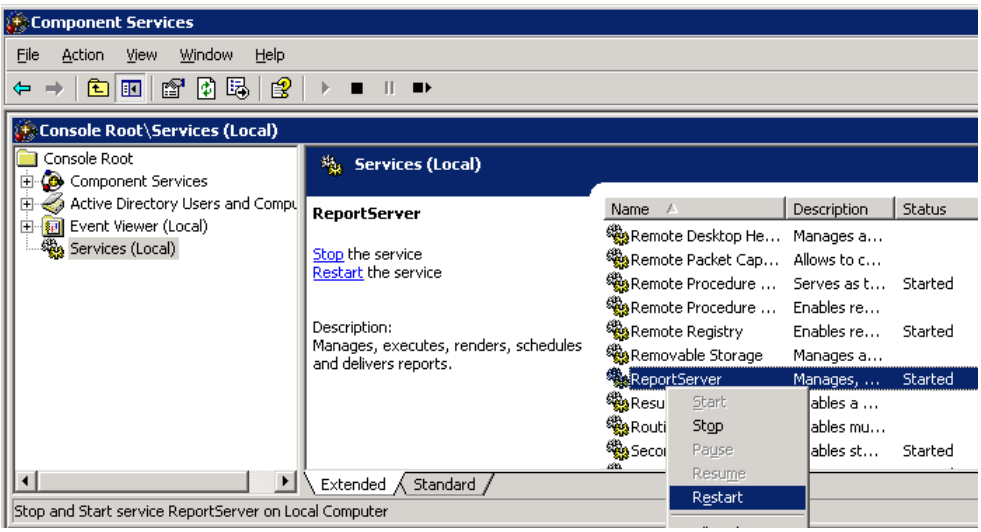
- On the Report Server Database dialog box, select Domain User Account from the **Credentials Type** dropdown. Then specify your local Administrator account. For example, `username=Adminstrator, password=<your password>, domain=<your machine name>`.



- Skip the Report Server Delivery Settings dialog.
- Set Licensing Mode according to your SQL Server licensing agreement.

2. Install SQL Server 2000 Reporting Services SP1.
3. Install SQL Server 2000 Reporting Services documentation update (optional).

4. Restart the ReportServer windows service.



5. From the **Start** menu, select **All Programs >Microsoft SQL Server > Reporting Services > Report Manager**.

6. Log on using the same credentials you plan to use when installing the Hercules Server.

7. When the Report Manager displays SQL Server Reporting Services, this indicates that the Reporting Services is correctly installed and active.

Note: If an Internet Explorer dialog box displays a message that content is blocked, click **Add**. Add the serer to the list of trusted sties and click **Close**.

Populate Hercules User Group on Reporting Machine

To set up access to Hercules Reports, your Windows account must be defined in the Hercules User Group on the machine where Reporting Services is installed. If the Hercules User Group doesn't exist, create it.

Note: If you plan to install the Hercules Server on the same machine with the SQL Server and Reporting Services, you can wait until after installing the Hercules Server to complete this task. Hercules Server installation creates the Hercules User group. However, doing this now enables you to immediately use the QuickStart after installing the Hercules Administrator console and run reports.

To set up access to Hercules Reports

1. Identify the machine where Reporting Services for Hercules is running. If you don't know the machine, ask your IT manager.
2. Log onto the machine where the Report Manager is installed as the local administrator.

3. From the Start menu, select A**ll Programs > Administrative Tools > Computer Management**.
4. Expand Local Users and Groups. Select **Groups.**
5. Do one of the following:
   a. If Hercules Users is not present, right-click Group under Local Users and Groups, and select New Group. For Group name, type **Hercules Users**.
   b. If Hercules Users is present, double-click **Hercules Users**.
6. Click **Add** to add the Windows accounts of Hercules Users to the Hercules User Group.
7. Enter the `<domain>\<username>` and click **Check Names**.
8. If requested, supply the credentials of an account authorized to add users.
9. Click **OK**.
10. Repeat for each user that is authorized to generate Hercules reports.
11. When all users have been added, do one of the following:
    a. If Hercules Users is a New Group, click **Create**, then click **Close**.
    b. If adding users to Hercules User Properties, click **Apply**, then click **OK**.
12. Close the Computer Management window.

Configure Enterprise Reporting

Hercules Enterprise Reporting provides reports on devices checking in to multiple Hercules Servers. The Hercules servers may have their Hercules databases on different SQL servers. To aggregate the data across servers, Hercules uses SQL replication services.

To configure enterprise reporting, create a domain account, such as `DOM6\HercSQL` with Hercules SQL database privileges. Add this account to each SQL server that hosts Hercules databases, grant Hercules SQL database rights to the account, and assign the same username and password. Machines with common credentials authenticate each other automatically. If the SQL servers involved in enterprise reporting are in different domains, create a trust relationship between the domains if one does not already exist.

Note: The account needed for the SQL Server cannot be LocalSystem because the LocalSystem on the current machine can't authenticate with the SQL Server on another machine.

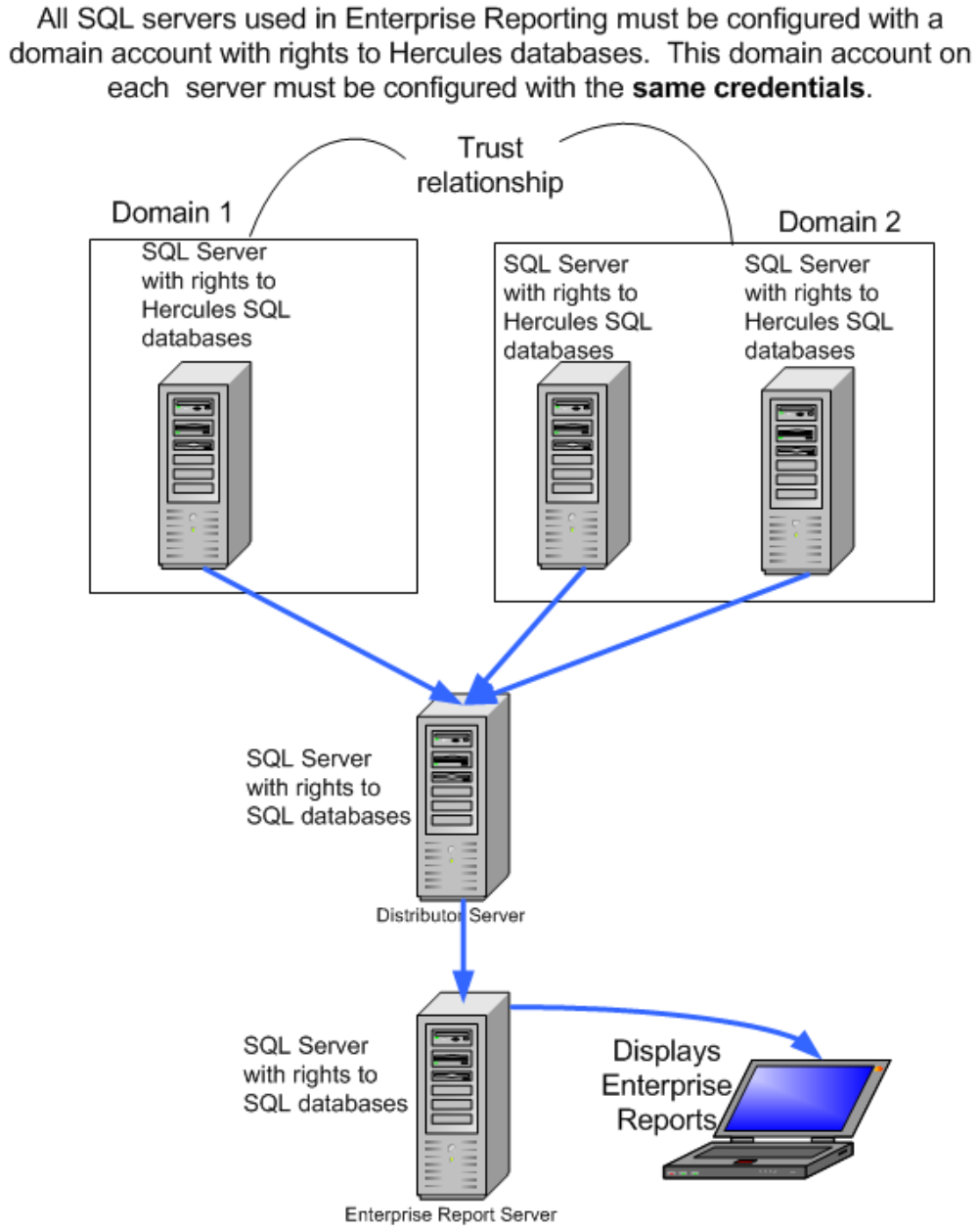


Figure 1-4. Enterprise Report Configuration

2. Installing Servers and Administrator

This chapter covers new installations and describes the following procedures:

- "Install v4.0 Servers in a Standalone Architecture" (page 2-2).
- "Install v4.0 Servers in a Distributed Architecture" (page 2-11).
- "Install the Hercules Administrator" (page 2-27).

Installation procedures differ depending on whether you install in a standalone or distributed environment. See Figure 1-1 on page 1-2.

- In a standalone environment, the Channel Server, and a Hercules Download Server are installed on the same machine as the Hercules Server.
- In a distributed environment, the Hercules Download Server and/or the Hercules Channel Server are installed on a machine other than the one where the Hercules Server is installed.

Select the Programs to Install

The minimal installation for v4.0 is one Hercules Administrator, one Hercules Server, one Channel Server, and one Hercules Download Server. This configuration supports at least 2000 clients. You can install the components in either a standalone configuration or a distributed configuration. With either configuration, you install only one Hercules Channel Server per zone; you can have more than one of any other Hercules component. It is recommended to install the Hercules Administrator on the machine with the Hercules Server.

When installing Hercules software for the first time where the three types of servers are distributed across multiple machines, you can install the servers in any order. The executable files you need, depend on whether you distribute the Hercules components across machines, and if so, how. The executable files you need for common configurations are shown on the following chart.

Machine 1	Machine 2	Machine 3	Executables
Hercules Server Channel Server Download Server			`setup.exe`

Hercules Server	Channel Server	Download Server	`setup.exe`
			`channelsetup.exe`
			`downloadsetup.exe`

Hercules Server Channel Server	Download Server		`setup.exe` `downloadsetup.exe`
Hercules Server Download Server	Channel Server		`setup.exe` `channelsetup.exe`

Install v4.0 Servers in a Standalone Architecture

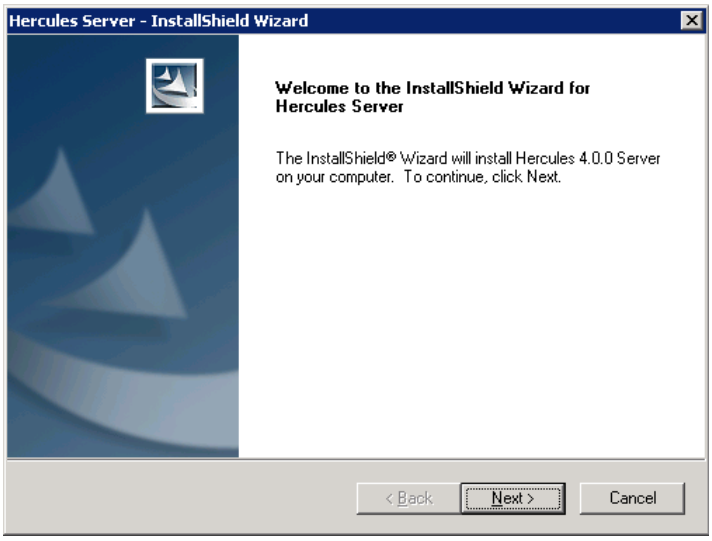
Use this procedure to install the Hercules Server, Hercules Channel Server, and Hercules Download Server on a machine that has no prior versions installed.

The installation is not completed until you reboot the machine and log in to the machine again.

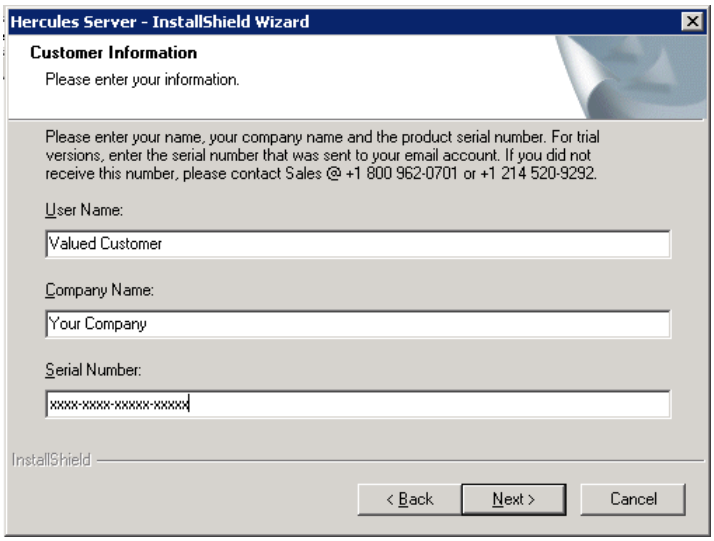
To install the Hercules Server in a standalone architecture

1. Ensure prerequisites are met. See "Pre-Installation Checklist" on page 1-6.
2. Log on to the selected server machine as a local administrator for that server.
3. Close all applications before beginning the installation.
4. Start the installation in one of the following ways:
   - If you downloaded the software, click the setup installation program icon.
   - If you have the Hercules CD, place it into the CD-ROM drive. Click the Windows Start button and select **Run**. Type **`<CDROM drive>:\Setup`** and click **OK** to start the Hercules Server InstallShield wizard.

   The Preparing to Install dialog box displays momentarily.
5. When the Welcome page displays, click **Next** to begin the installation of the Hercules Server.



6. On the Customer Information page, type your name, your company's name, and the product serial number printed on the CD sleeve. Then click **Next**.

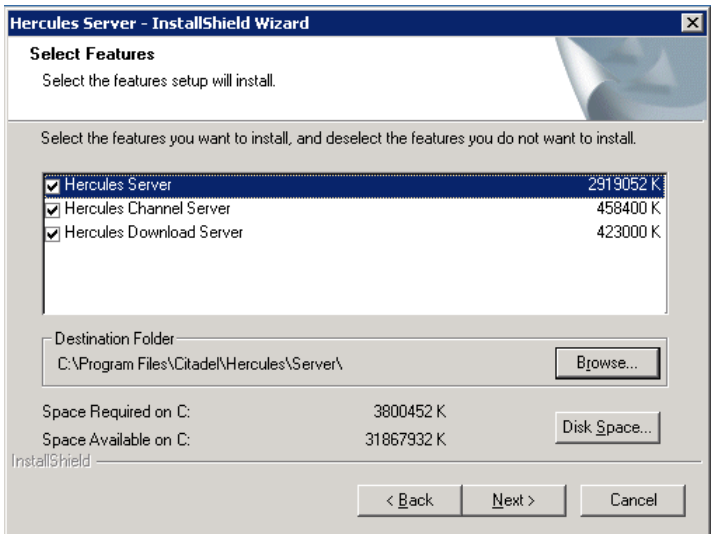


7. Carefully read the terms and conditions in the Software License Agreement. To accept the agreement and continue with the installation, click **I accept the terms of the license agreement** and click **Next.**

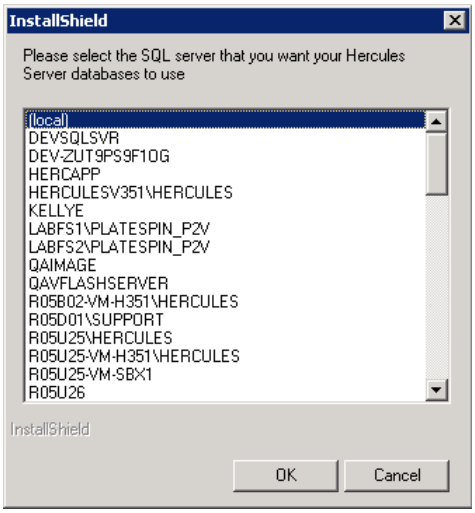
8. When the Select Features page displays, determine whether you want to install only the Hercules Server, the Hercules Server and one of the other servers, or all three servers.

Server	Description
Hercules Server	The main Hercules server.
Channel Server	Server that facilitates communication between the Hercules Server and the Hercules Download Servers
Hercules Download Server	Server that downloads patches and other files from third-party websites on the Internet.

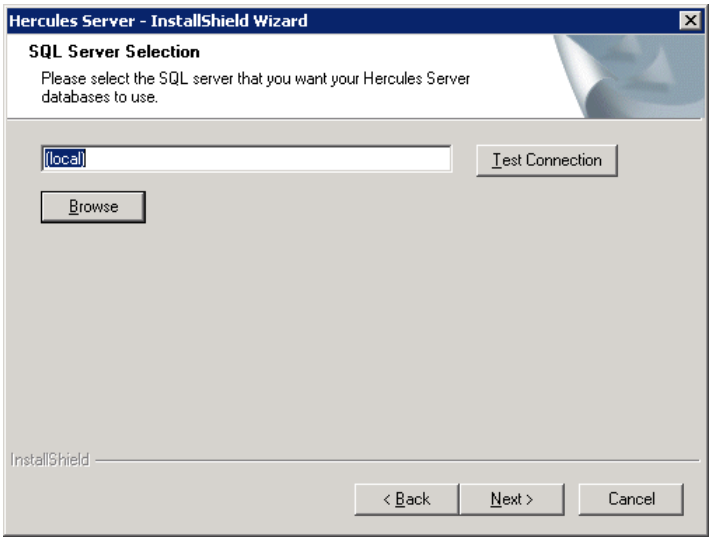
9. Accept the default to install all features now, and click **Next**.



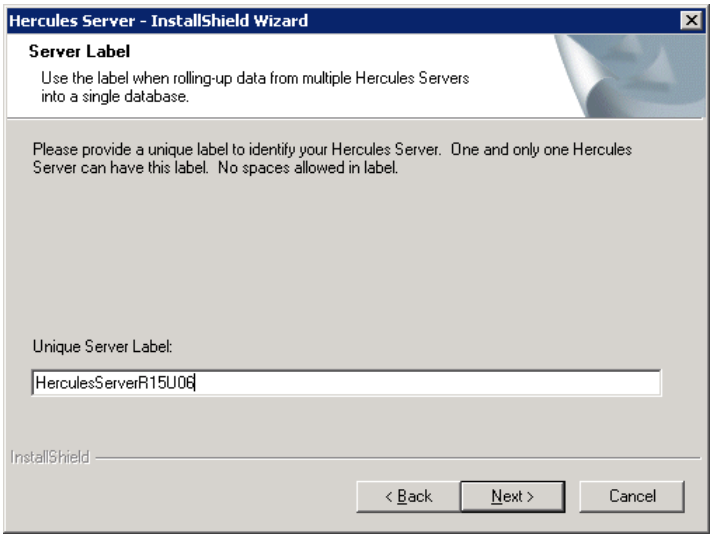
10. When the SQL Server Selection window displays, click **Browse** to open a list box listing SQL servers. Select the server the Hercules Server databases are to use, then click **OK**.



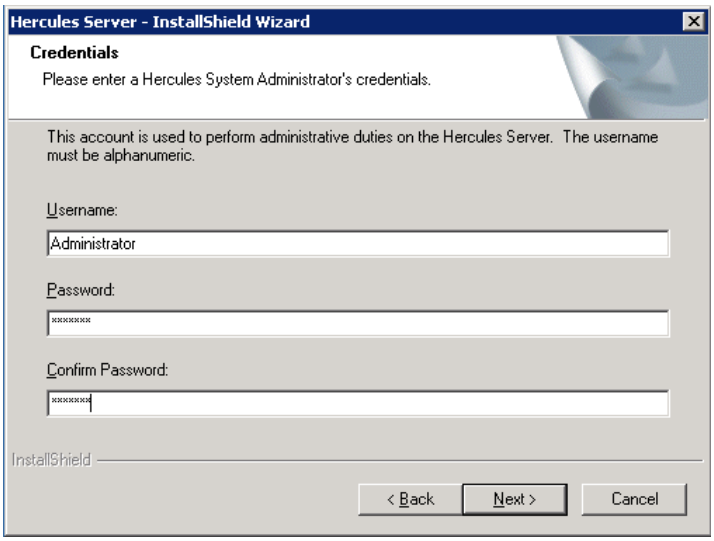
11. Verify the entry you selected is displayed, then click **Test Connection**.



12. Click **OK** to the confirmation message that the connection was successful. Then click **Next**.
13. For **Unique Server Label**, accept the default or type a one-word label (no spaces) to uniquely identify this Hercules Server, then click **Next**.

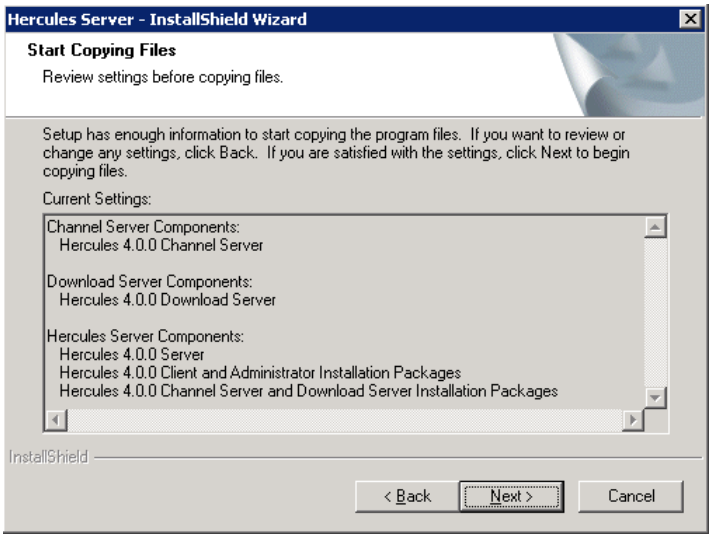


14. Supply your selected **Username** and **Password** for access to the specified Hercules Server you are installing. In the **Confirm Password** text box, type the selected password for that user on the specified Hercules Server. Click **Next**.

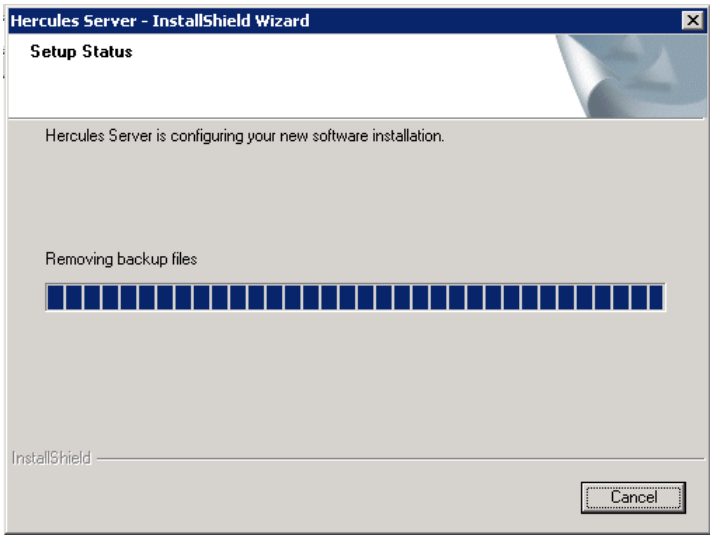


15. Review the packages to be installed and then click **Next**. The listed Installation Packages are what enables the Installer to set up the directory structures on the server. Under `Program Files > Citadel, Hercules`, three folders are created: `Channel Server`, `Download Server`, and `Server`.

    The Hercules 4.0.0 Client Installation Package is installed in the following folder under `Server`:
    `Web\HerculesServer\ Installers\Client`

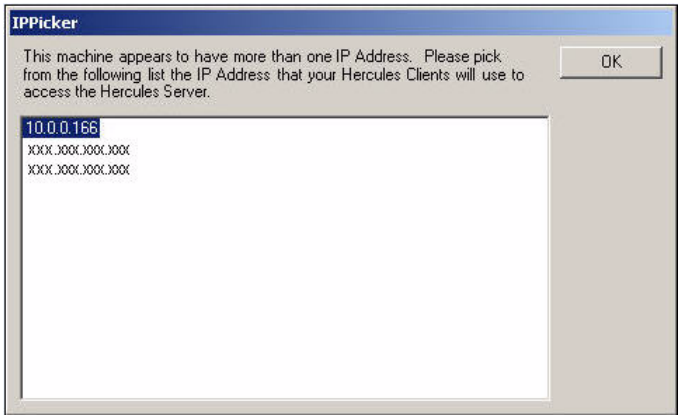


16. When the setup begins, the Installer installs the components listed for copying. The final setup process is registering the product. Wait while setup is in progress.

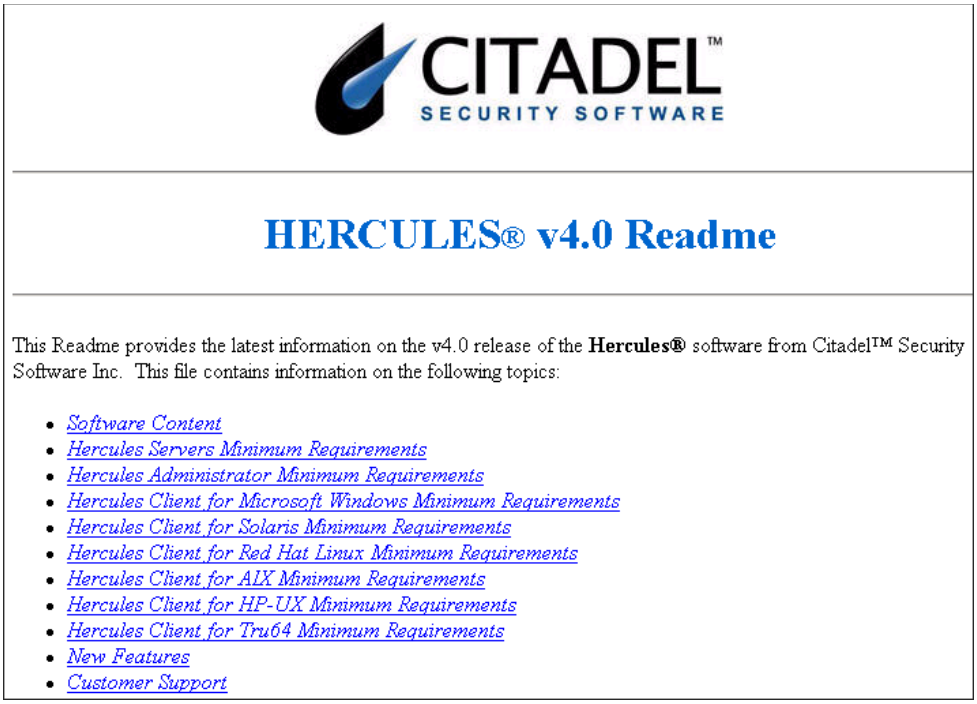


17. Please wait while the installer finishes configuring your system. You can monitor the progress of configuring the Hercules Channel Server, Hercules Download Server, and Hercules Server.

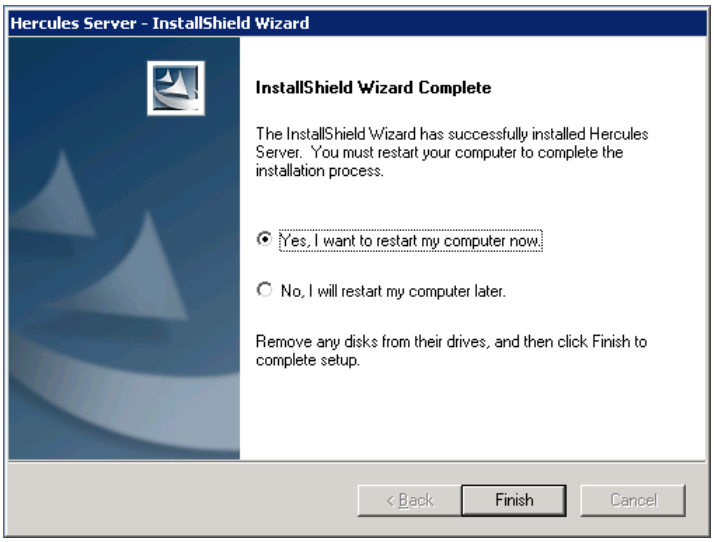
18. If an IPPicker dialog box displays, the server machine on which you are installing the Hercules software has multiple IP addresses (either virtual addresses or multiple NICs). Select the IP address for the Hercules server from the IPPicker dialog box.



19. When the Readme HTML page displays, review its contents and close the file.

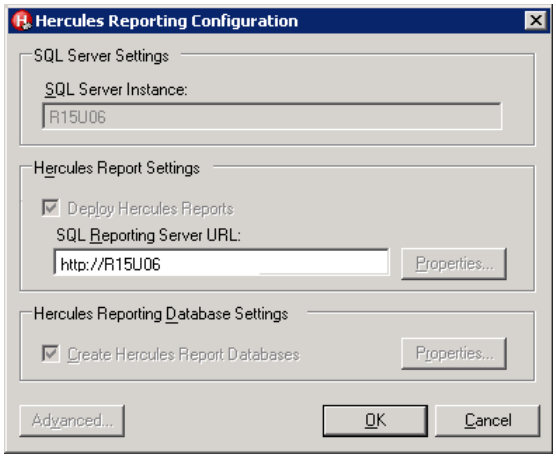


20. When the Hercules Server setup complete page displays, select **Yes** to restart your computer now and then click **Finish**.



21. Wait while the reboot occurs. Then, log back on to the Windows with the same credentials you used when logging on to do the installation, then click **OK**. The Hercules processing dialogs display momentarily.

22. When the Hercules Reporting Configuration window displays, verify the SQL Reporting Server URL. If it is not the URL for the server to use for Hercules Reporting recommended by your IT manager, change it and click **OK**. (You can accept the default now and change this later from the Hercules Administrator console using Edit Server Registration.) The Hercules Report Configuration Status displays.



23. When the Installation succeeded message displays, read it and then click **OK**.

Caution: Wait a full 15 minutes or until hard drive activity has stopped before continuing. SQL is setting up replication databases for reporting. If this process is interrupted, you may be unable to run Reports.

24. Continue with "Install the Hercules Administrator" (page 2-27).

Install v4.0 Servers in a Distributed Architecture

This section provides step-by-step instruction for installing the v4.0 servers on separate machines using separate executables. Procedures include:

- "Install the Hercules Server" (page 2-11).
- "Install the Hercules Channel Server" (page 2-19).
- "Install the Hercules Download Server" (page 2-23).

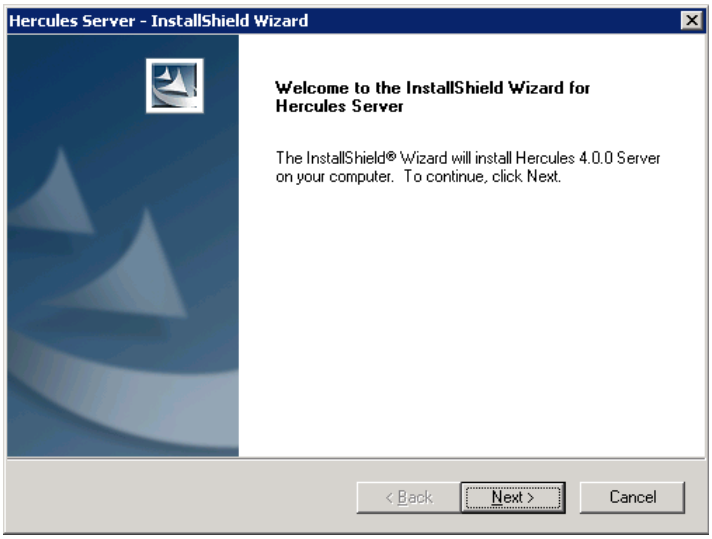
Install the Hercules Server

Use this procedure to install the Hercules Server on a machine that has no prior versions installed.

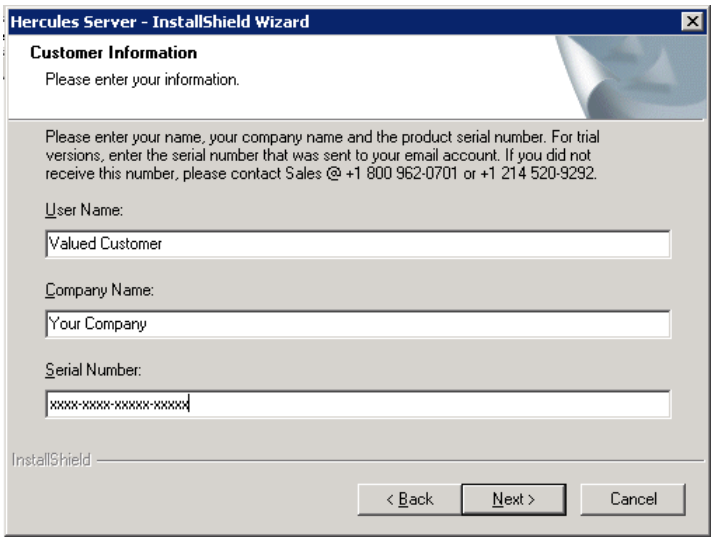
To install the Hercules Server in a distributed architecture

1. Ensure prerequisites are met. See "Pre-Installation Checklist" on page 1-6.
2. Log onto the selected server machine as a local administrator for that server.
3. Close all applications before beginning the installation.
4. Initiate the installation process in one of the following ways:
   - If you downloaded the software, click the setup installation program icon.
   - If you have the Hercules CD, place it into the CD-ROM drive. Click the Windows Start button and select **Run**. Type **`<CDROM drive>:\Setup`** and click **OK** to start the Hercules Server InstallShield wizard.

   The Preparing to Install the Hercules Server dialog box displays momentarily.
5. When the Welcome page displays, click **Next** to begin the installation of the Hercules Server.

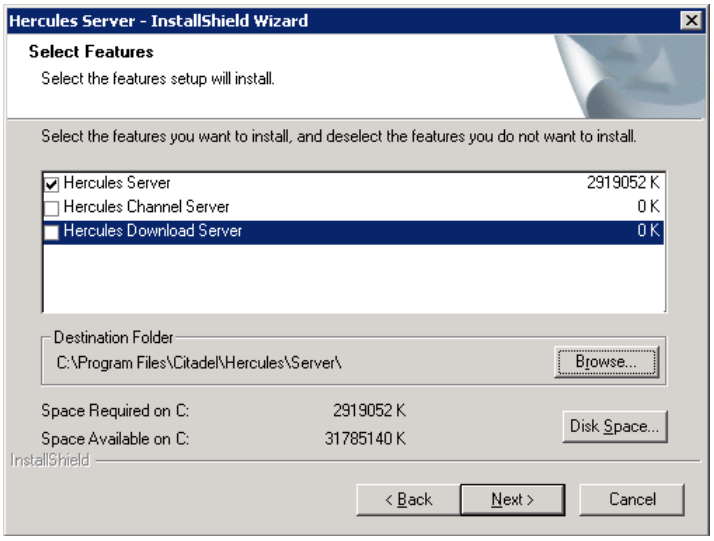


6. On the Customer Information page, type your name, your company's name, and the product serial number printed on the CD sleeve. Then click **Next**.

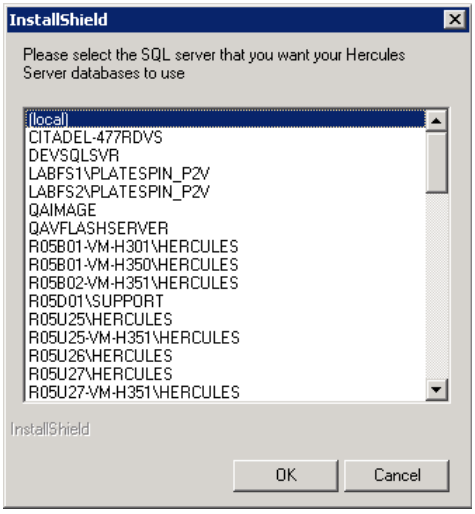


7. Carefully read the terms and conditions in the Software License Agreement, and then click **Yes** to accept the agreement and continue with the installation.

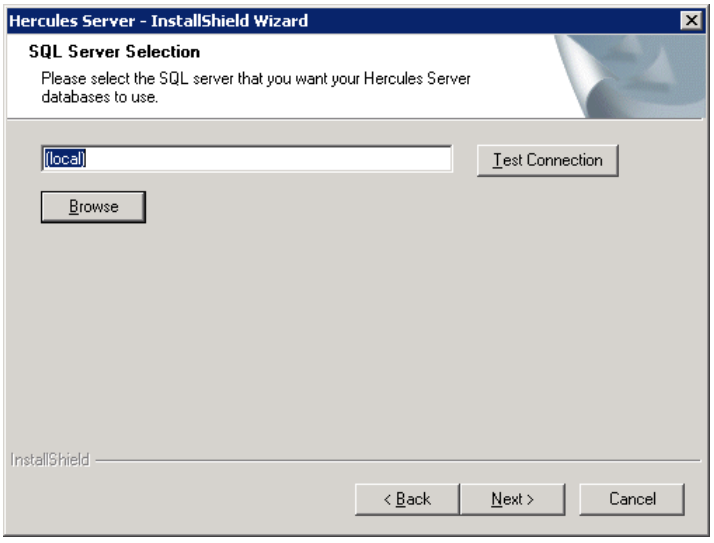
8. Examine the Select Features page. This is where you specify that you want to install only the Hercules Server on this machine. Leave the Hercules Server feature selected. Click to clear the check box for the Hercules Channel Server. Click to clear the check box for the Hercules Download Server. Then, click **Next**.



9. When the SQL Server Selection window displays, click **Browse.**
10. Select the SQL server that this Hercules Server's databases is to use. If the SQL server is installed on the current machine, select **`(local)`**. Click **OK**.



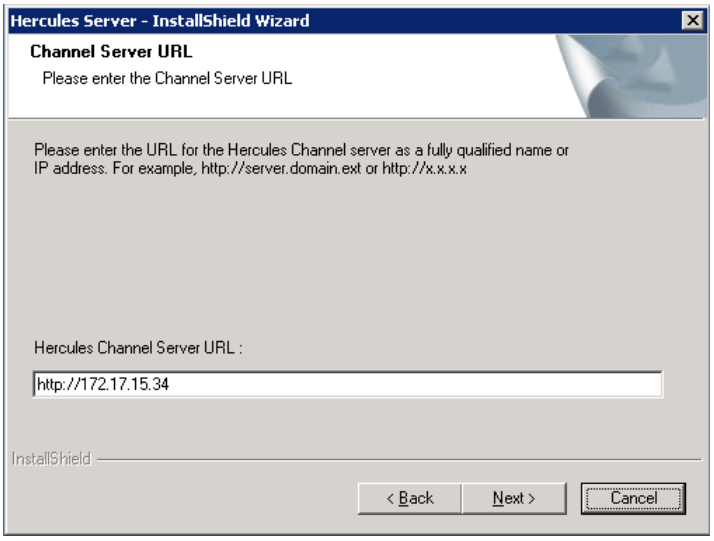
11. When the SQL Server Selection window re-displays with your selection, click **Test Connection**. Click **OK** at the confirmation, Successfully established database connection. Click **Next**.



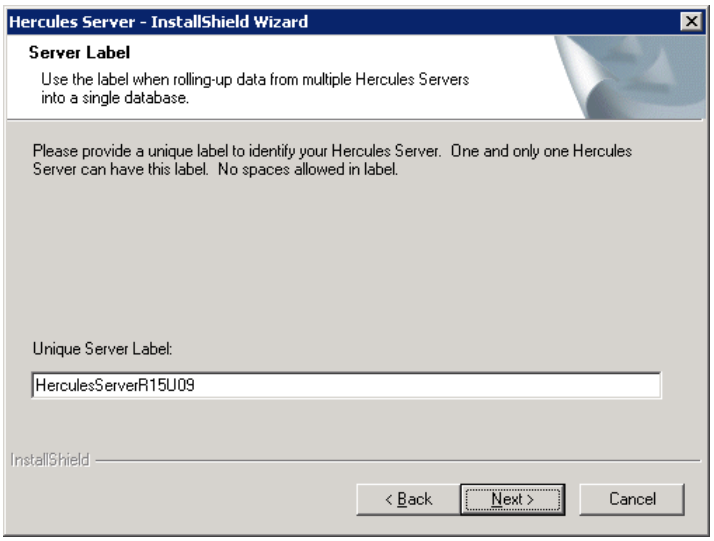
12. Since you did not select to install the Channel Server, the Channel Server URL page displays. In **Hercules Channel Server URL**, type the URL for the Channel Server, for example,

    `http://R15U34.lab.citadel.com or http://172.17.15.34`

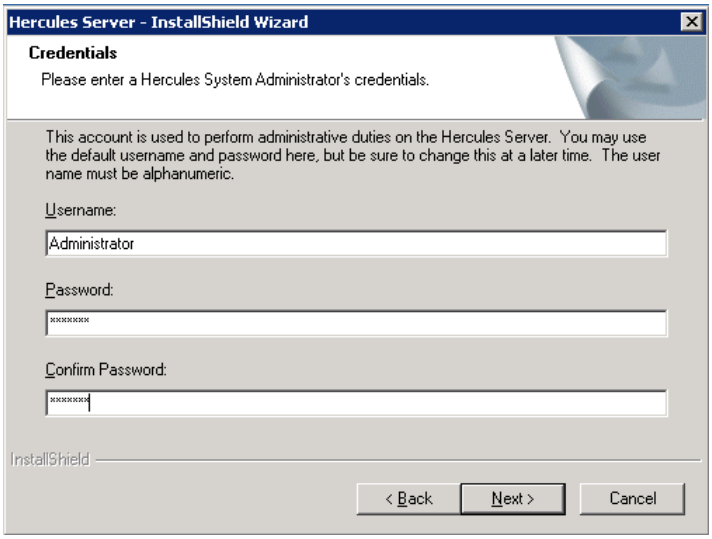
13. Click **Next**. The Channel Server should be behind your firewall on a private IP subnet and not Internet-accessible.



14. For **Unique Server Label**, type a one-word label (no spaces) to uniquely identify this Hercules Server, then click **Next**.

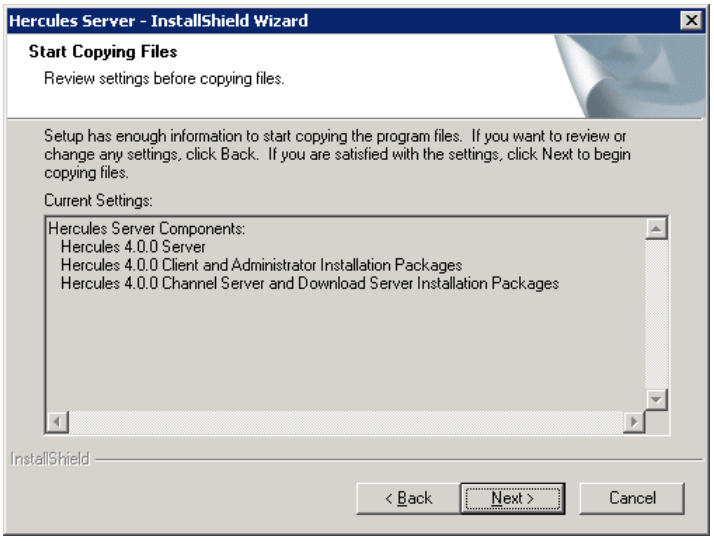


15. Enter the credentials for a Hercules System Administrator. Then click **Next**.

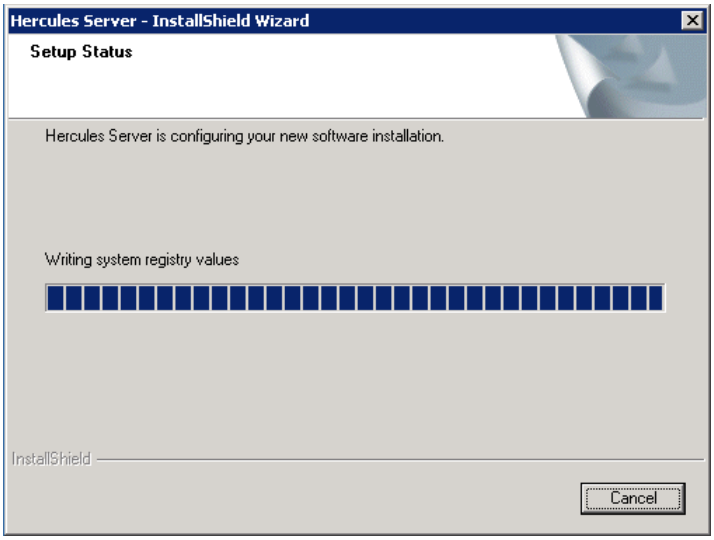


16. Review the packages to be installed and then click **Next**. The listed Installation Packages are what enables the Installer to set up the directory structures on the server. For example, the Client Installation Package is installed as the following directory:

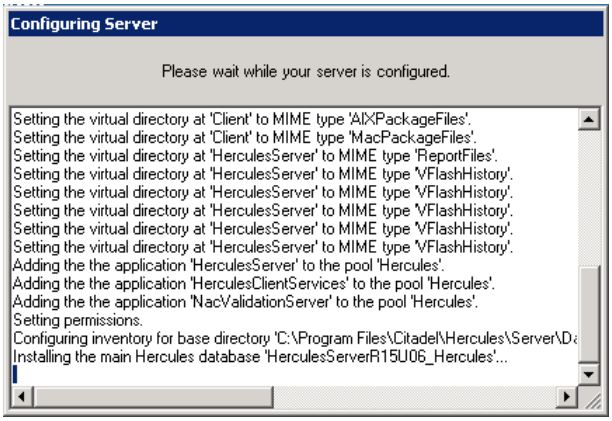
    `C:\Program Files\Citadel\Hercules\Web\Installers\Client`



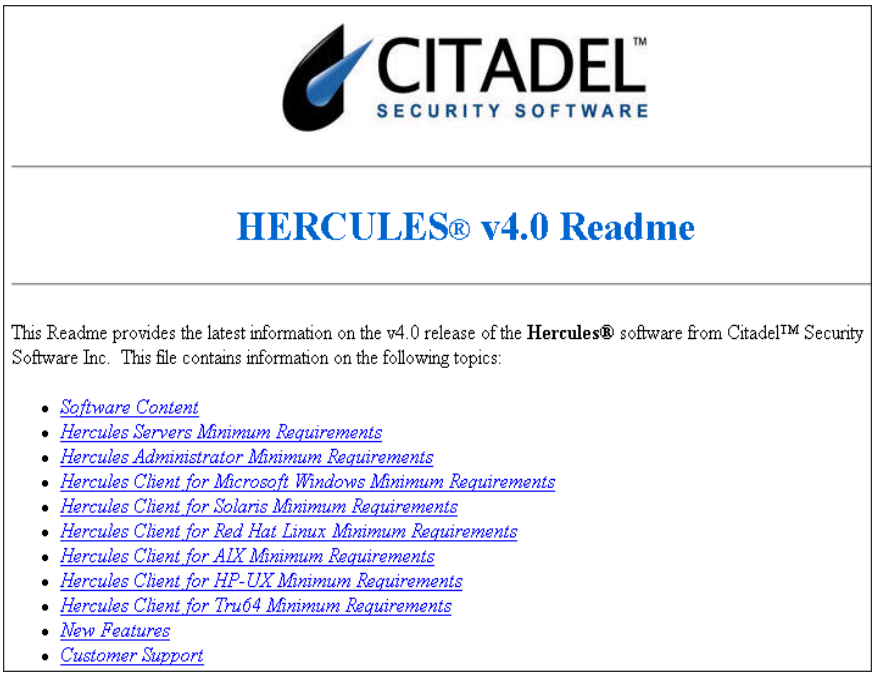
17. The setup status displays.



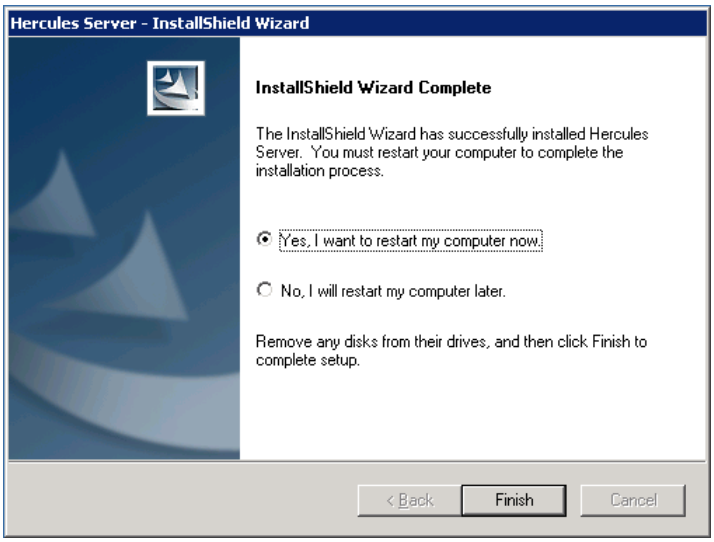
18. Now that all selected server files have been installed, the setup program begins the process of configuring the Hercules Server. The configuration process creates the Hercules database and configures the IIS web server components and other objects used by the Hercules Server.



19. When the Readme HTML page displays, review its contents and close the file.

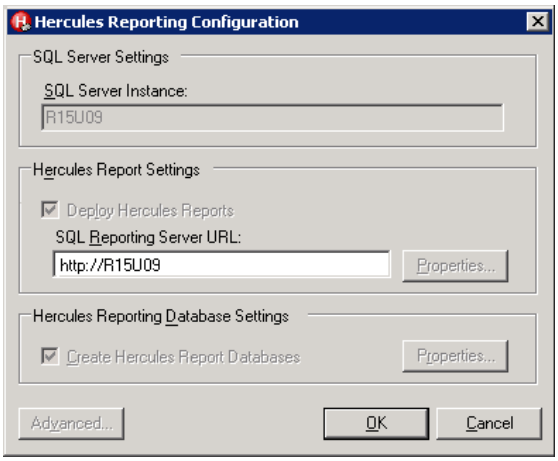


20. When the Hercules Server setup complete page displays, select **Yes** to reboot now and then click **Finish**.



21. Wait while the reboot occurs.
22. Log back on to the Windows with the same credentials you used when logging on to do the installation, then click **OK**. A processing dialog displays momentarily.

23. When the Hercules Reporting window displays, verify the SQL Reporting Server URL. If the displayed URL is not the URL recommended by your IT manager as the server to use for Hercules Reporting, change it and click **OK**.



24. When the Installation succeeded message displays, click **OK**.

Caution: Wait a full 15 minutes or until hard drive activity has stopped before continuing. SQL is setting up replication databases for reporting. If this process is interrupted, you may be unable to run Reports.

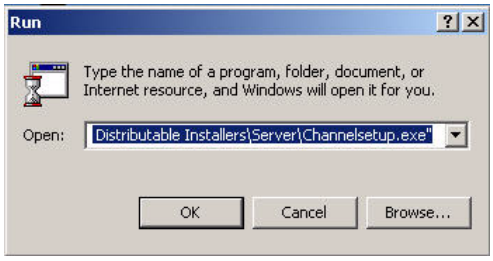
25. Continue with "Install the Hercules Channel Server" (page 2-19).

Install the Hercules Channel Server

Use this procedure to install the Hercules Channel Server. Each Hercules zone must have one and only one Hercules Channel Server.

To install the Hercules Channel Server in a distributed architecture

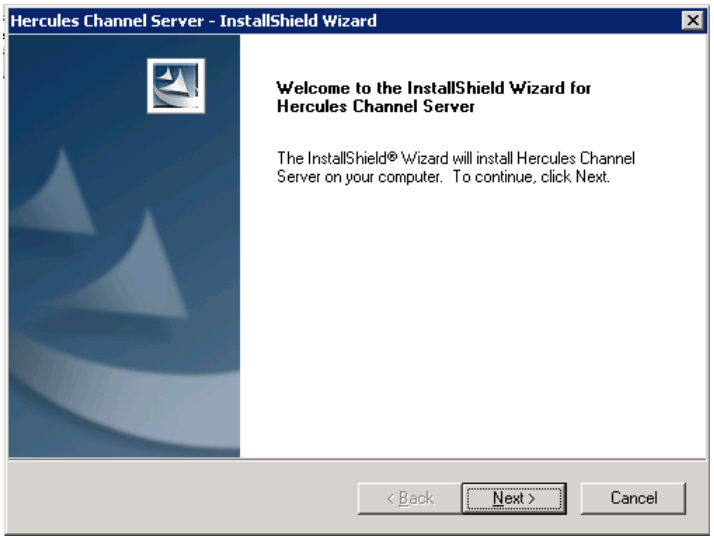
1. Log onto the selected server machine as a local administrator for that server.
2. Close all applications before beginning the installation.
3. Begin the installation as follows.
   a. Place the Hercules CD into the CD-ROM drive, click the Windows **Start** button and select **Run**. Type the drive letter of the CD-ROM, click **Browse**, and navigate to
   `Hercules Distributable Installers\Server`
   b. Select **`Channelsetup.exe`**
   c. Click **Open**. Then, click **OK**.



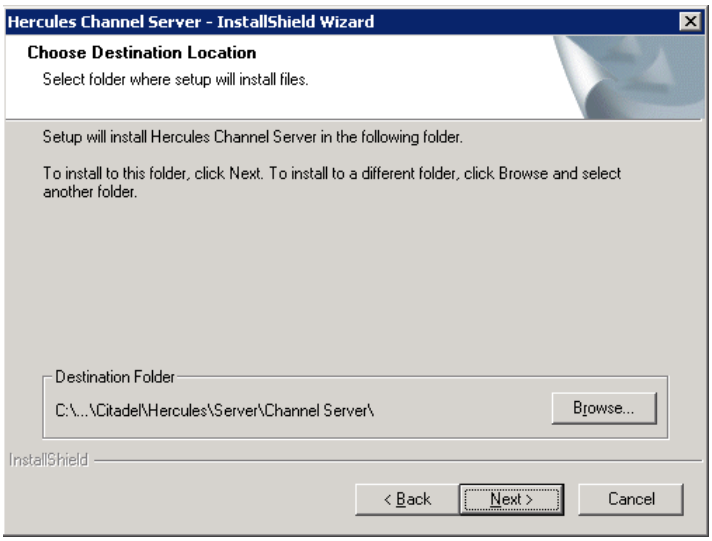
Note: Alternatively, download or copy the **`Channelsetup.exe`** file to your hard disk, then double-click the **`Channelsetup`** icon.

The Preparing to Install page displays momentarily.

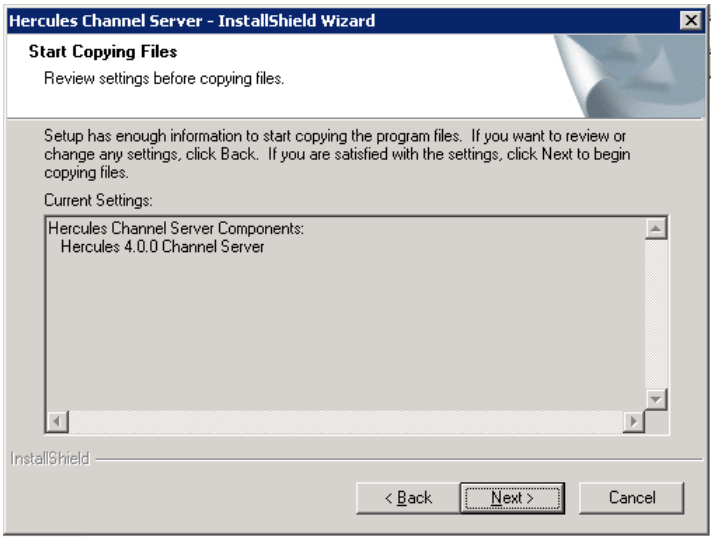
4. When the Welcome page displays, click **Next** to begin the installation of the Channel Server.



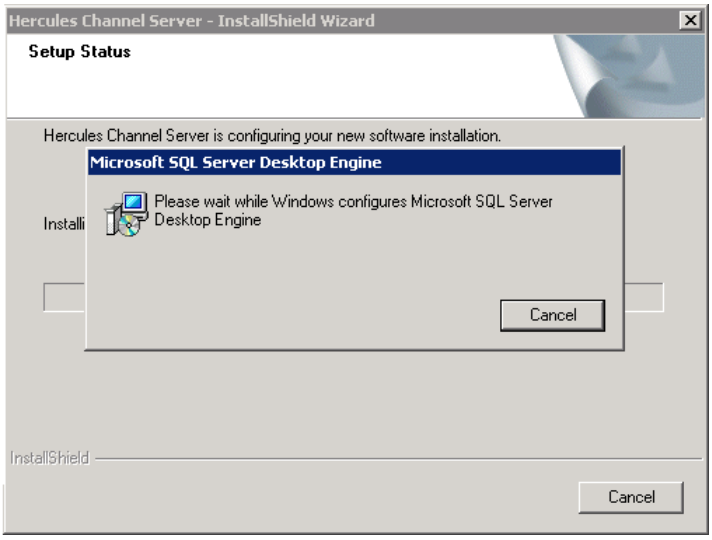
5. When the Choose Destination Location page displays, notice the default directory in which the Hercules Channel Server is to be installed. To accept the default, click **Next**. Or, click **Browse** to specify a different path and then click **Next**.



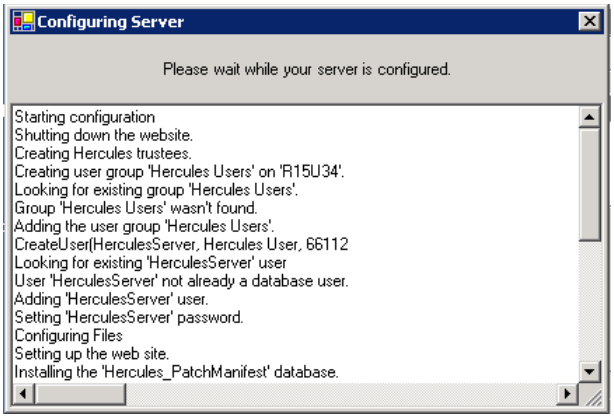
6. Review the packages to be installed and then click **Next** to copy the Channel Server and its components.



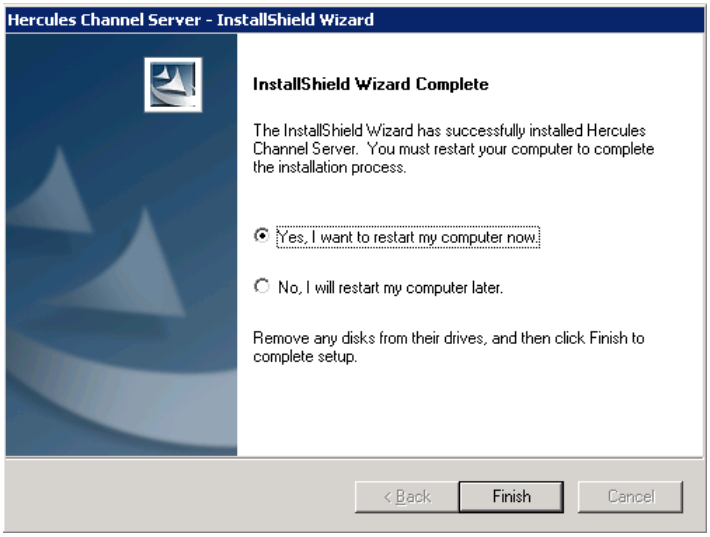
7. Wait while setup is in progress.



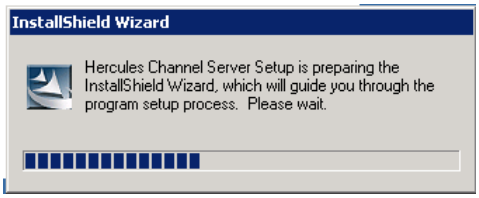
8. After the Hercules Channel Server files have been installed on the server, you can monitor the process of configuring the Channel Server on the Configuring Channel Server dialog box.



9. When the Hercules Channel Server Wizard Complete displays, accept the default to restart the computer and click **Finish.**



10. Wait while the reboot occurs.
11. Log back on to the Windows with the same credentials you used when logging on to do the installation, then click **OK**. The installation program completes the installation.



12. Continue with the procedure, "Install the Hercules Download Server" (page 2-23).

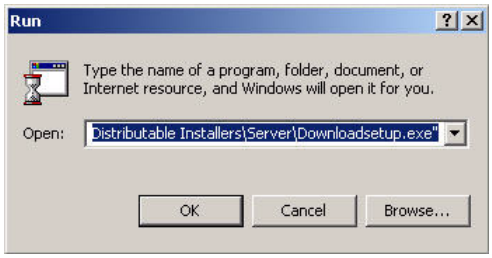
Install the Hercules Download Server

For each Hercules Download Server you need, use the following guidelines to perform the installation.

To install the Hercules Download Server in a distributed architecture

1. Begin the installation as follows.
   - Log on to the selected server machine as a local administrator for that server.
   - Close all applications before beginning the installation.
   - Place the Hercules CD into the CD-ROM drive. Click the Windows **Start** button and select **Run.** Type the drive letter of the CD-ROM, click **Browse**, and navigate to

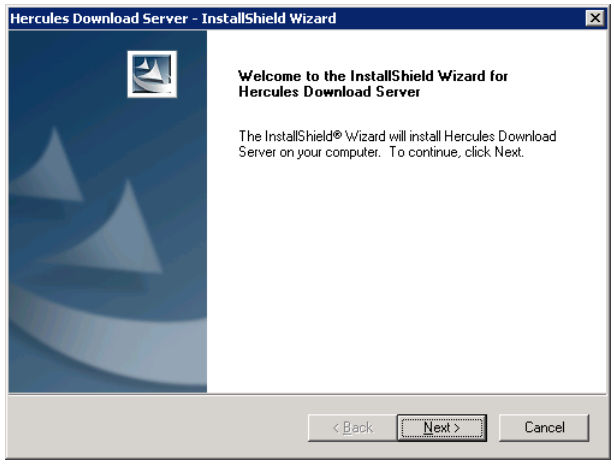
     `Hercules Distributable Installers\Server`
     Select **`Downloadsetup.exe`** and click **Open**. Then click **OK.**



Note: Alternatively, copy **`Downloadsetup.exe`** to your hard disk, and double-click the **Downloadsetup** icon.

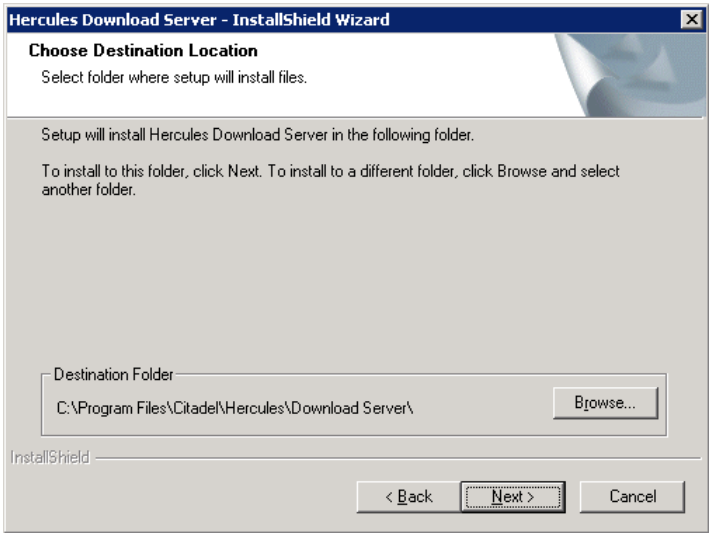
The Preparing to Install page displays momentarily.

2. When the Welcome page displays, click **Next** to begin the installation of the Hercules Download Server.

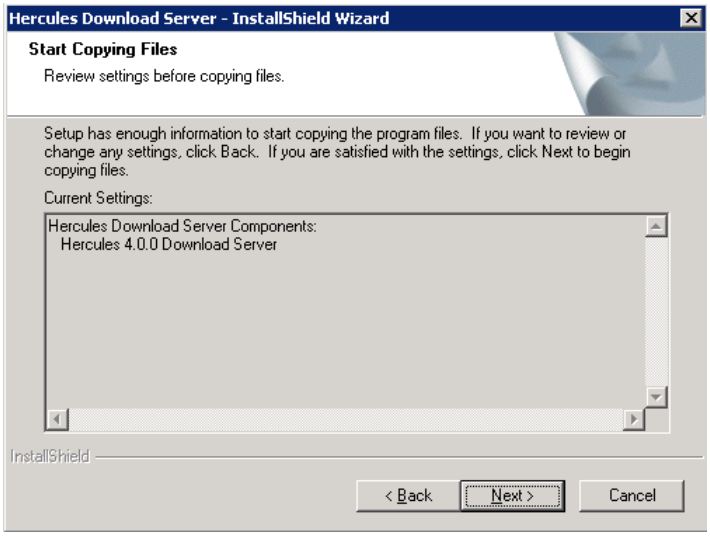


3. To accept the default installation folder, click **Next**. The Hercules Download Server will be installed in the default directory:
   `C:\Program Files\Citadel\Hercules\Download Server\`

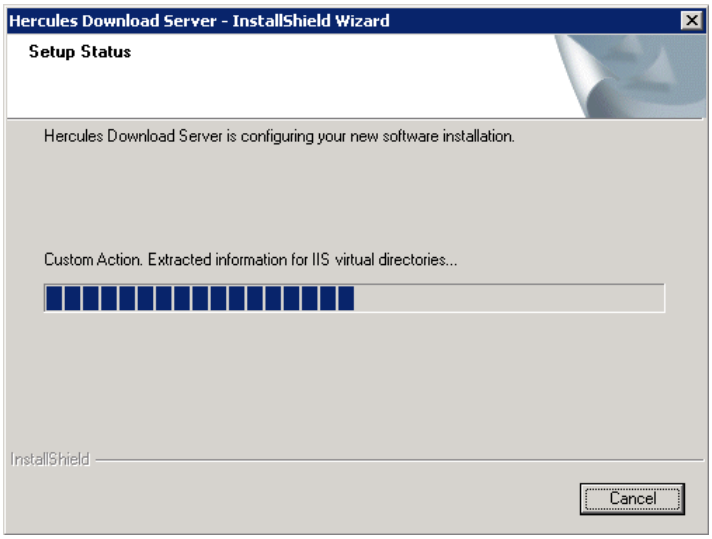
   Or, click **Browse** to specify a different path and then click **Next**.



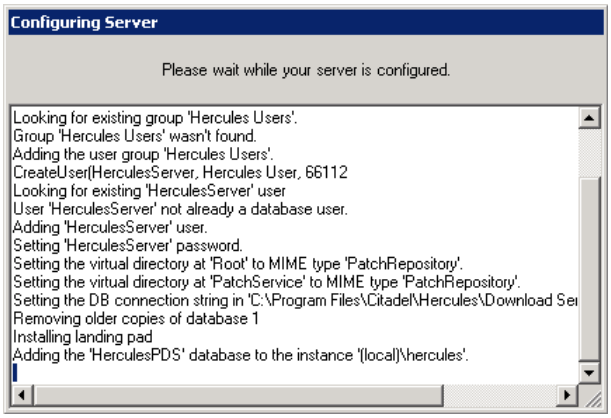
4. Review the packages to be installed and then click **Next** to install the Hercules Download Server and its components.



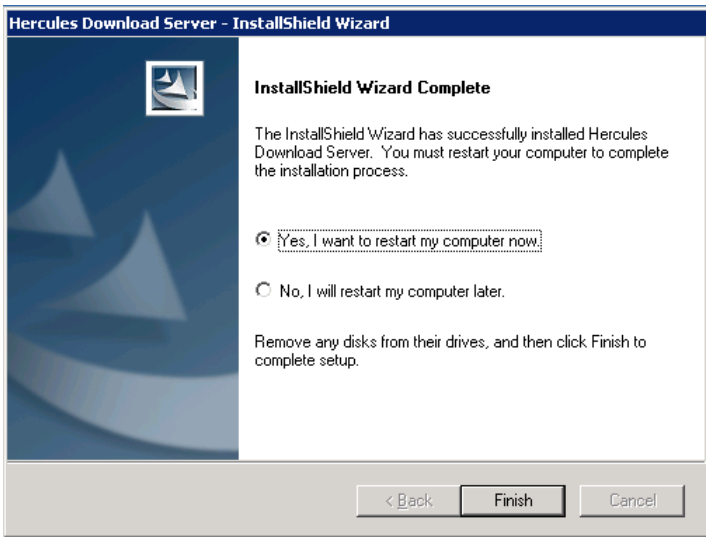
5. When the Setup Status displays, just wait until the process completes.



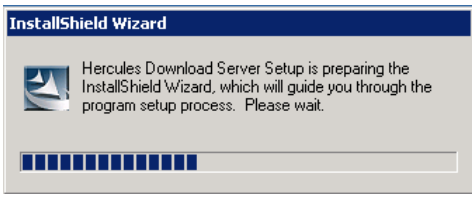
6. After the Hercules Download Server files have been installed on the server, the configuration process begins. Please wait while the installation process configures your system. You can monitor the configuration process to learn what happens in each step.



7. When the Hercules Download Server installation completes, accept the default to restart the computer now and click **Finish**.



8. Wait while the reboot occurs.
9. Log back on to the Windows with the same credentials you used when logging on to do the installation, then click **OK**. The installation program silently completes the installation. Wait until the setup completion finishes.



10. Continue with "Install the Hercules Administrator" (page 2-27)

Install the Hercules Administrator

Install the Hercules Administrator on the server machine with the Hercules Server or on a remote machine.

If you already have the Hercules Administrator installed on your server machine, you must remove it first with the **Add/Remove Programs** in the Control Panel.

Before beginning the installation, verify you meet the minimum requirements. See "Hercules Administrator Installation Minimum Requirements" (page 1-11).

To install the Hercules Administrator console

1. Log on to the machine with the Hercules server or any remote Windows machine with the same credentials you used to install the Hercules server.

   Note: The user name from this login was added at installation time as a Hercules User with the role, Hercules System Administrator. This account must be used to add the *next* user. If you add a user with the role, Hercules System Administrator, that user can add other users.

2. Access the Hercules Component Installation page in one of the following ways, depending on where you are logged on:

   - If logged on to the machine with the Hercules server, click **Start** and select **All Programs >Hercules > Hercules Installers** to open the Hercules Component Installations page.
   - If logged on to a remote machine, open Internet Explorer, type this URL, and click Go to open Hercules Component Installations:

     `http://<servername>/HerculesServer/`

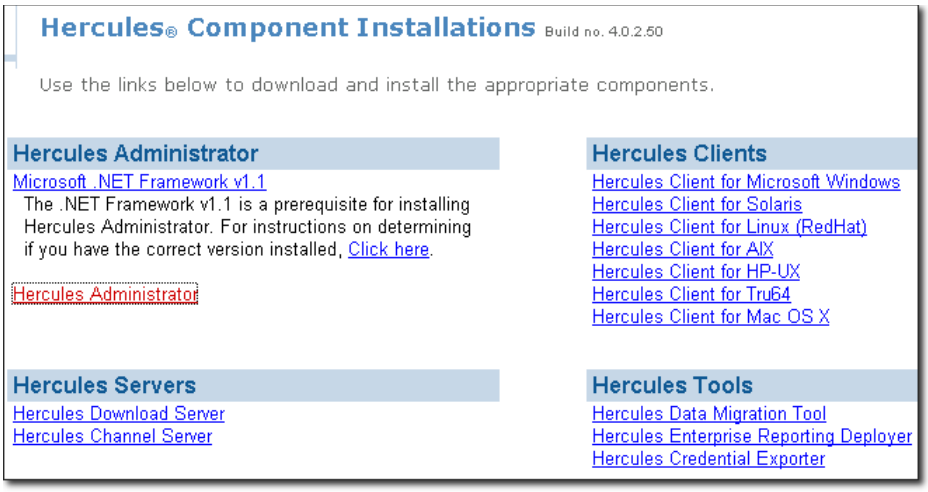
     where `<servername>` is the fully qualified host name, host name, or IP address of the Hercules Server.

3. If you are logged on to a Windows Server 2003, continue with Step 6. Otherwise, continue.

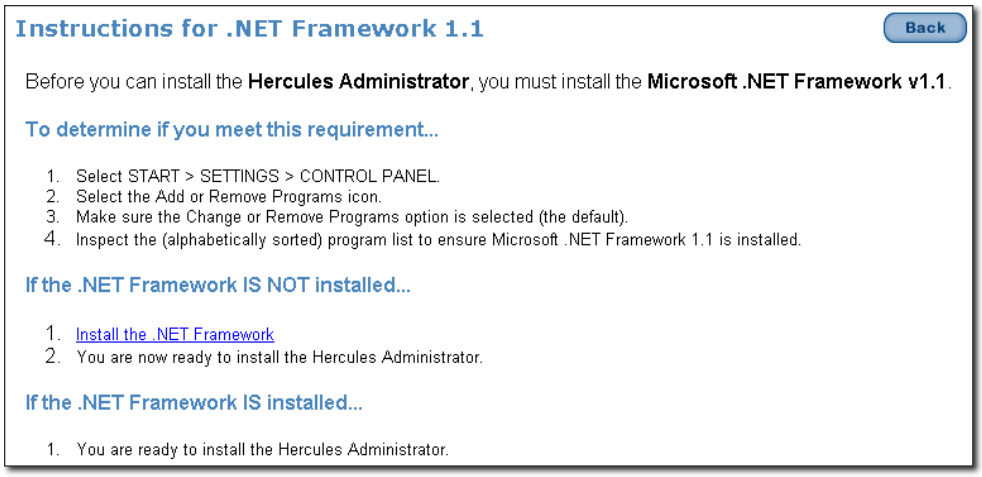
4. Do one of the following:

   - If you do not know whether you have .NET installed, click the **Click here** link and continue with Step 5.
   - If you know you do not have .NET installed, click **Microsoft .NET Framework v1.1** to complete the installation, then continue with Step 6.

- If you know you do have .NET installed, continue with Step 6.



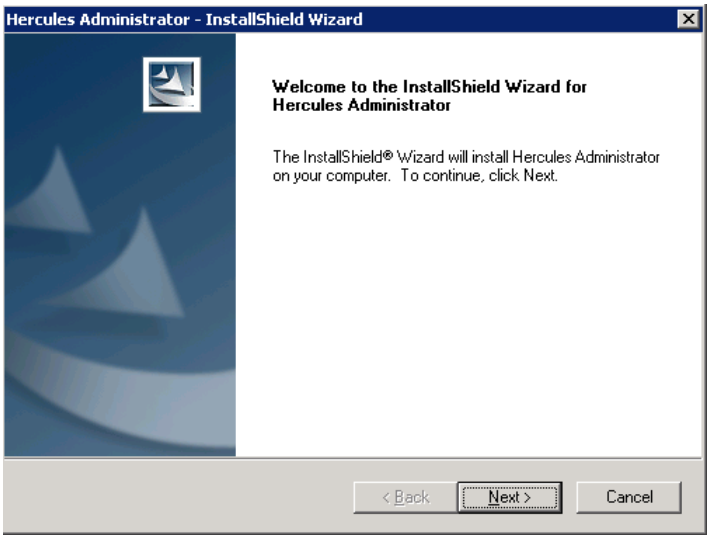
5. Follow the instructions to determine whether you have .NET Framework v1.1 installed by examining the Add or Remove Programs list. If the .NET framework is not installed, click **Install the .Net Framework** to initiate the download of dotnetfx.exe and complete the installation of this prerequisite software. Then continue with Step 6.



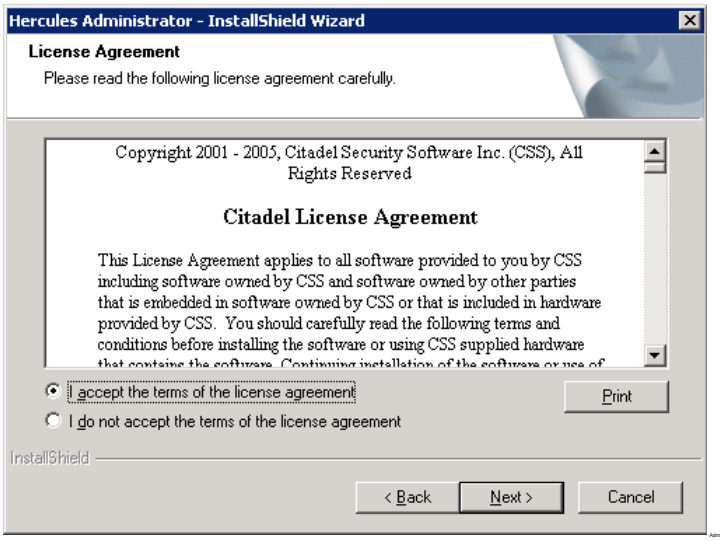
6. Select **Hercules Administrator** to display the Windows File Download dialog box. Click **Open** or **Run** to run the setup utility directly or click **Save** to download the setup utility to the local machine. If you select Save, navigate to the target location and double-click the executable to start it.
7. If a security warning displays, click **Yes**.

   The Preparing to Install the Hercules Administrator page displays momentarily.

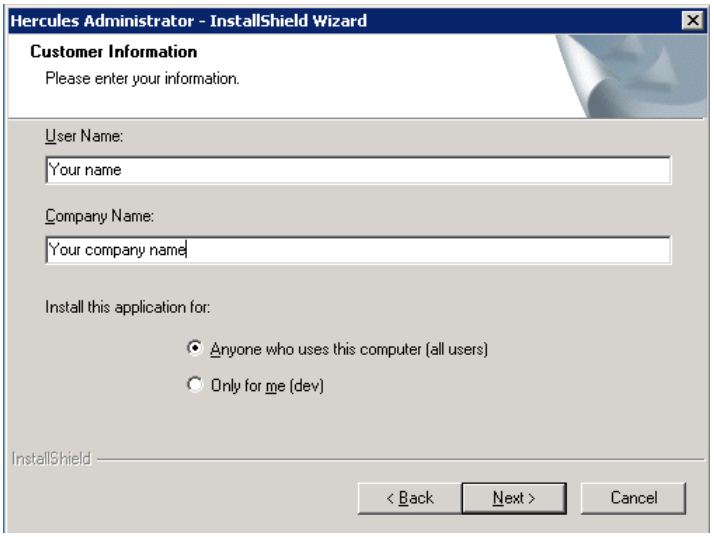
8. When the Hercules Administrator Welcome displays, click **Next.**



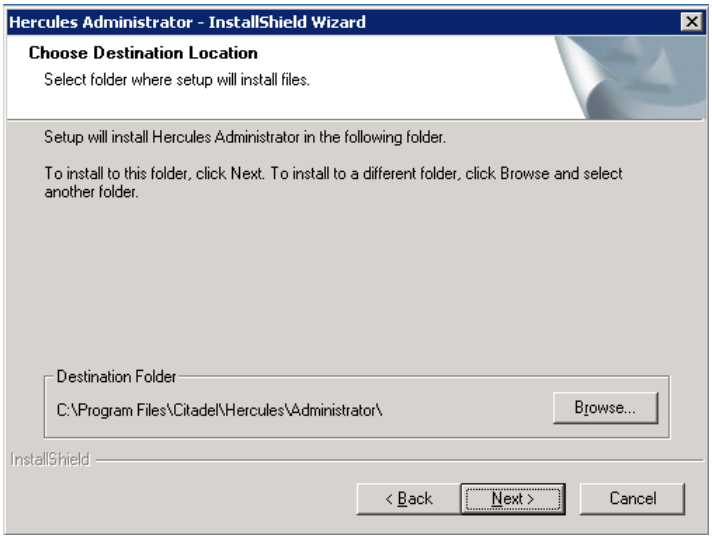
9. To accept the terms of the license, select **I accept the terms of the license agreement**, and then click **Next**.



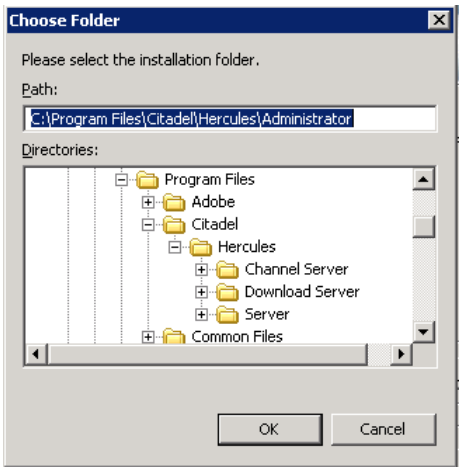
10. In the Customer Information page, type **User Name** and **Company Name**. Select install **Only for me** or **Anyone**, depending on who is allowed access to the application based on login profile. Then click **Next**.



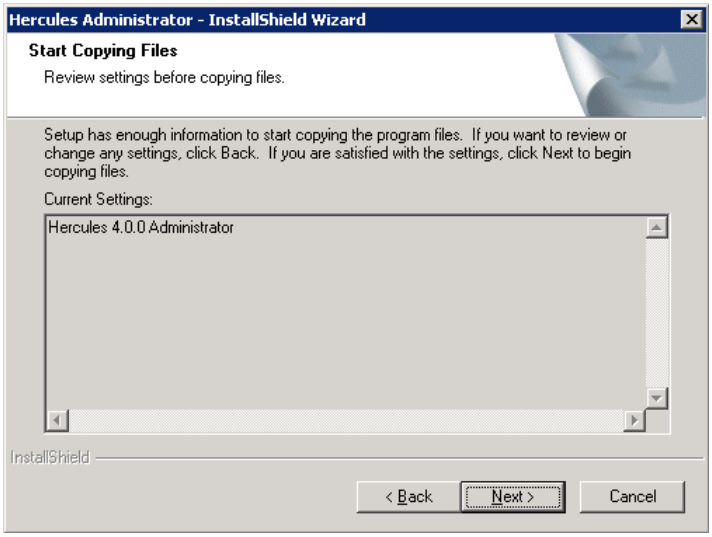
11. In the Choose Destination Location page, do one of the following:
    - Click **Next** to select the Destination Folder default.



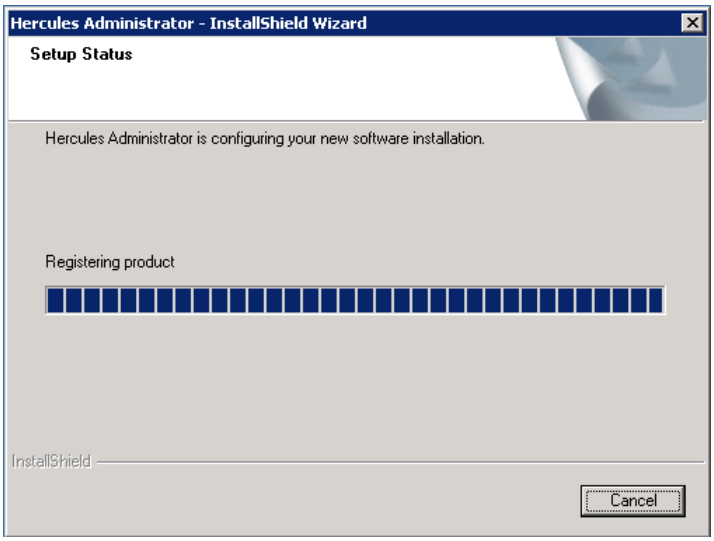
- Click **Browse** and select a different directory path location, click **OK** to close this window, and then click **Next**.



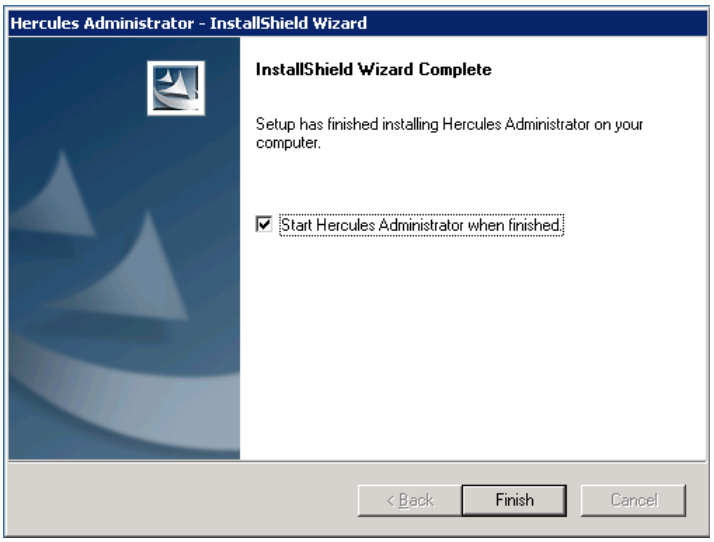
12. The Start Copying Files page displays the current settings. Click **Next**.



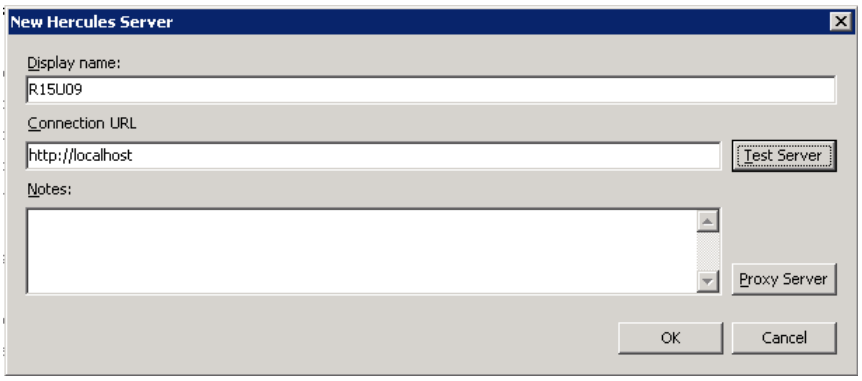
13. While the Installer sets up the Hercules Administrator, you can monitor the setup steps as they are being performed.



14. To complete the Hercules Administrator installation, accept the option to start the Hercules Administrator and click **Finish**. The New Hercules Server dialog box displays, where you add the new server.



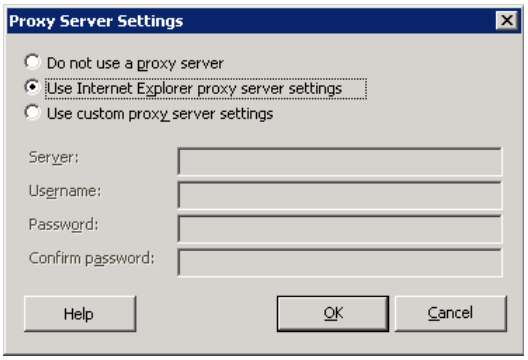
15. For **Display Name**, type the name of the server as you want it displayed. For **Connection URL**, type one of the following:
    - If installing with the Hercules Server, type **`http://localhost`**
    - If installing remotely, type **`http://<server_name_or_IP_address>`**
    - If using SSL, type **`https://`** followed by the common name on the Hercules Server certificate for **Connection URL**. The common name is usually the fully qualified name. The syntax is: **`https://<server>.<domain>.<ext>`**.



To edit these settings at any time, select **Edit Server Registration** from the right-click menu.

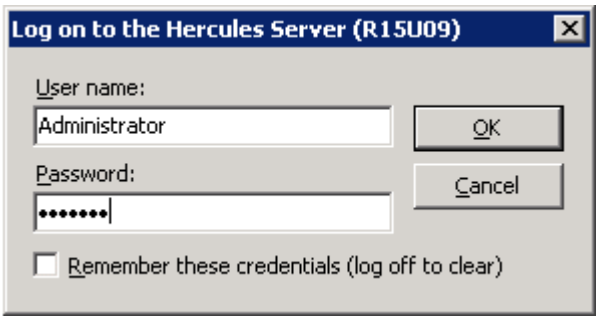
Note - This entry configures a server on the Hercules Administrator console.

16. If using a proxy server, click **Proxy Server** to open Proxy Server Settings. The default is to not use a proxy server. If using one, either select **Use Internet Explorer proxy server setting** or select **Use custom Proxy server settings** and identify the server name and credentials. Click **OK**.



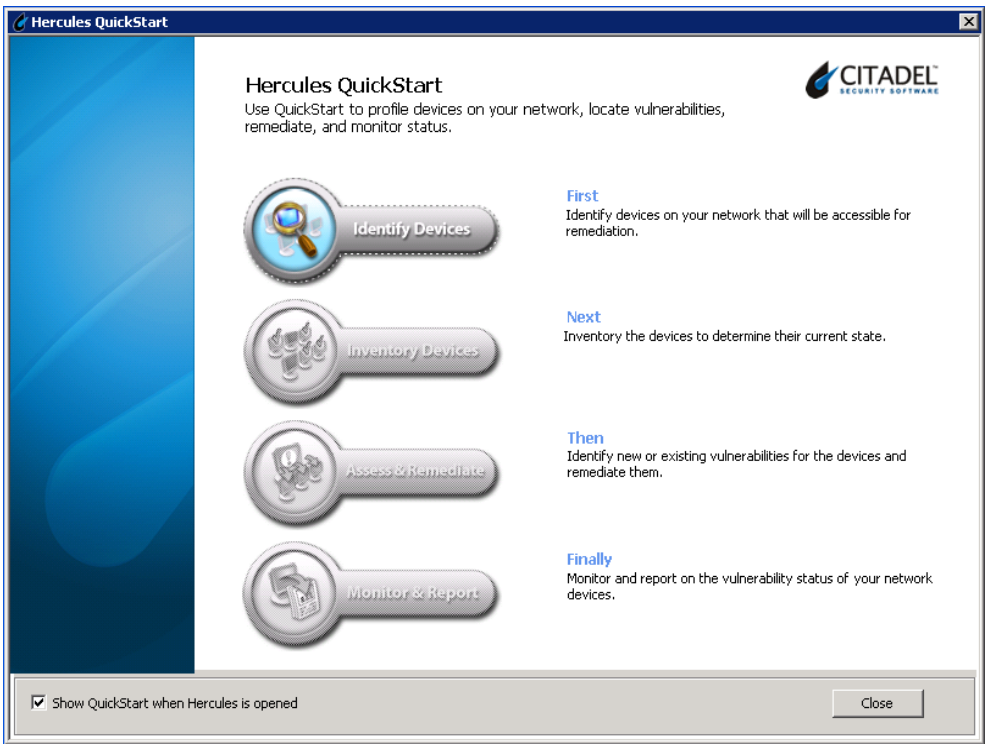
17. Click **Test Server**. Click **OK** to the message, Successfully connected to the Hercules server. Click **OK** to save the new server settings, close the dialog box, and open the Log on to the Hercules Server dialog box.

18. Type the name with which you logged on to the local host in the **User name** text box. Type the associated password in the **Password** text box. These must be the same credentials used when installing the Hercules Server. Optionally, select **Remember these credentials (log off to clear)**.



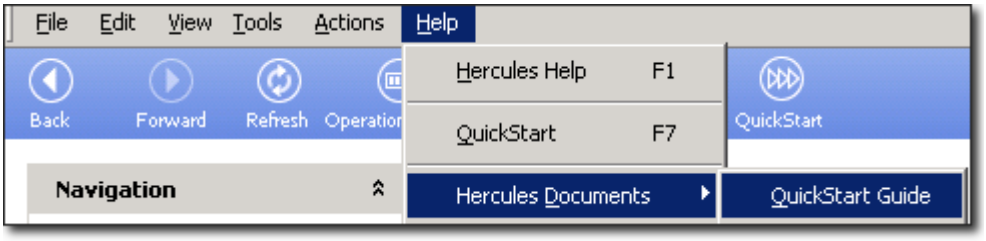
Note - The username and password you enter here are automatically added to the Users and Security - Users tab of the Hercules Administrator console.

19. Click **OK** to save the new Hercules Server credential information and open Hercules QuickStart. The accompanying *Hercules Quick Start Guide* provides instructions to help you discover devices for QuickStart remediation, enforce a policy, and produce a report showing remediation results.



20. From the Hercules QuickStart window, continue in one of these ways:

- To use the Hercules QuickStart right away with online help, click **Identify Devices** on the Hercules QuickStart home page. After completing the QuickStart, return to Chapter 3, "Completing Post Installation Setup" on page 3-1 for suggestions on tasks to do next.
- To use the Hercules QuickStart right away with a printed copy of the *Hercules Quick Start Guide*, click **Close** to close the Hercules QuickStart and display the toolbar of the Hercules Administrator console. Select **Help > Hercules Documents > QuickStart Guide** to display the PDF of the guide. Optionally, print the guide. The click the **QuickStart** toolbar button to resume the QuickStart. After completing the QuickStart, return to Chapter 3, "Completing Post Installation Setup" on page 3-1 for suggestions on tasks to do next.



- To defer using the Hercules QuickStart, click **Close** to close the Hercules QuickStart and continue with Chapter 3, "Completing Post Installation Setup" on page 3-1.

3. Completing Post Installation Setup

After you install the Hercules servers and the Hercules Administrator, you may want to do some initial setup. If so, consider the following suggestions.

Perform these tasks from the server where the Hercules servers are installed.

- "Complete Setup for Remediating Microsoft IE 6.0 and Office 2000" (page 3-1).
- "Grant User Access to the Channel Server and Download Server" (page 3-2).
- "Complete Hercules Reporting Setup" (page 3-6)

Perform these tasks from a Hercules Administrator console:

- If you did not add your account to Client Management Services (CMS) during the QuickStart, do so now so that you can manage the Hercules Client devices. See "Add Administrator-Privileged Accounts for Managing Hercules Clients" (page 3-7).
- Optionally, set up Hercules user accounts with roles you select or design. See "Grant User Access to the Hercules Server and Assign Roles" (page 3-10).

  Note: Anyone who logs on to the Hercules Administrator console with the credentials you used when you installed Hercules can use all licensed Hercules features.
- Schedule frequent downloads of the latest information from Citadel. See "Initialize V-Flash" (page 3-12).

Complete Setup for Remediating Microsoft IE 6.0 and Office 2000

This section addresses:

- "Create the Network Install Package for Microsoft IE 6.0"
- "Create the Network Install Package for Microsoft Office 2000"

Create the Network Install Package for Microsoft IE 6.0

To ensure that all Hercules remedies execute properly and to finalize your Hercules installation, create the installation package for Internet Explorer Service Pack 1. Without this package, most of the remedies included for Microsoft Internet Explorer vulnerabilities will not complete successfully. To obtain directions for creating the installation package, select **Hercules Documents > IE Installation Package** from the Help menu.

Create the Network Install Package for Microsoft Office 2000

Set up the installation package for using Hercules functionality to apply service packs to Microsoft Office 2000 systems. To obtain directions for creating the installation package, select **Hercules Documents > Office Installation Package**.

Grant User Access to the Channel Server and Download Server

At installation, the Windows userid of the installer of the Hercules Channel Server is added to the Local Group, *HerculesChannelServerUsers*. Likewise, the Windows userid of the installer of each Hercules Download Server is added to the respective Local Group, *HerculesDownloadServerUsers*.

Until explicitly authorized, no user but the installer can successfully connect to the Hercules Channel Server website or the Hercules Download Server website. The procedures addressed in this section describe how to give additional users access to these web sites.

To connect to the Hercules Channel Server or a Hercules Download Server through the Hercules Administrator or directly though a browser, the logged on user must first be authenticated as having a valid Windows userid. Then, the logged on user must be authorized to access the server. For the authorization process to succeed for a given user, you must add either their individual Windows userid or the name of a Windows group to which they belong to the associated Local Group.

Members of the *HerculesChannelServerUsers* Group can manage and configure the Hercules Channel Server. The Hercules Channel Server maintains the File Download Catalog, a list of URLs used by the Hercules remedies to install patches, applications scripts, and other files. The Hercules Channel Server also coordinates activities on the Hercules Download Servers. Users with access to the Hercules Channel Server can manage existing File Download entries used by Hercules remedies, add new ones, and edit the proxy server settings used by the Hercules Channel Server to communicate with the Hercules Download Servers.

Members of the *HerculesDownloadServerUsers* Group can manage and configure the local Hercules Download Server. Hercules Download Servers download and store files—including patches, applications, and documents for the Hercules Channel Server. User with access to the Hercules Download Server can view the status of download activities on the server and edit settings used by this server to download and store files.

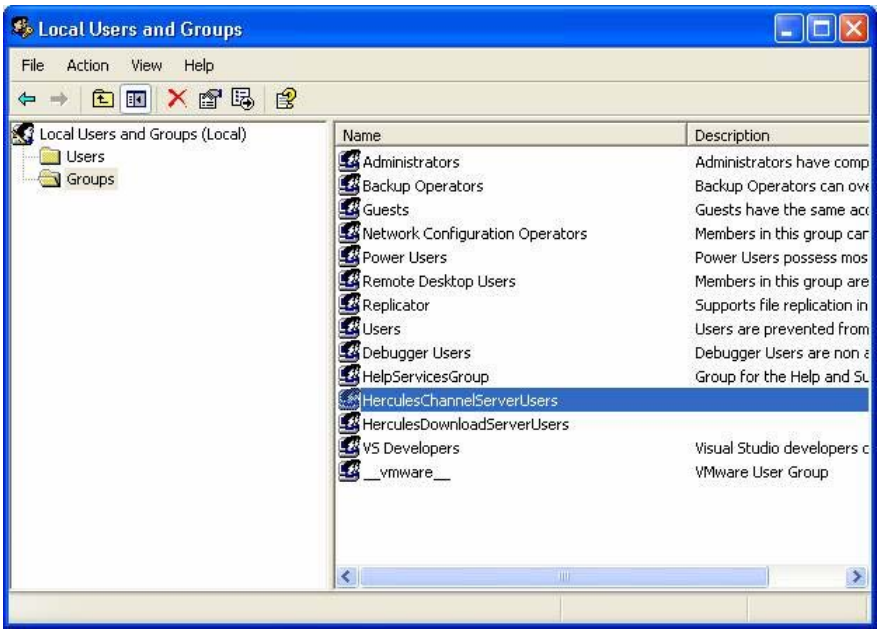
Add Users or Groups to HerculesChannelServerUsers Local Group

Only Windows users that are members of the *HerculesChannelServerUsers* Local Group, that is, local to the Hercules Channel Server, are given access to the Hercules Channel Server web site.

Add Members to HerculesChannelServerUsers in Windows 2000 Server

To add a user or group to the HerculesChannelServerUsers Local Group

1. Log on to the server where the Hercules Channel Server is installed.
2. From the **Start** menu, select **Settings > Control Panel**.
3. Select **Administrative Tools > Computer Management.**
4. Expand **Local Users and Groups** and click **Groups**.



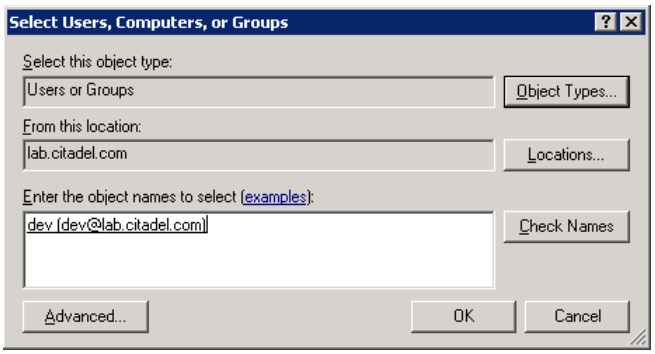
5. Open **HerculesChannelServerUsers**. Click **Add** to open Select Users, Computers, or Groups.
6. If the displayed location is not correct, click **Locations**. Select the domain for the user or group to be authorized to configure the Hercules Channel Server. Click **OK**.
7. Type the name of the group or user to be authorized in the text box and click **Check Names**.
8. Click **OK**.

Add Members to HerculesChannelServer Users in Windows Server 2003

To add a user or group to the HerculesChannelServerUsers Local Group

1. Log on to the server where the Hercules Channel Server is installed.
2. From the **Start** menu, select **All Programs > Administrative Tools > Computer Management.**
3. Expand **Local Users and Groups** and click **Groups**.
4. Open **HerculesChannelServerUsers**. Click **Add** to open Select Users, Computers, or Groups.

5. If the displayed location is not correct, click **Locations**. Select the domain for the user or group to be authorized to configure the Hercules Channel Server. Click **OK**.
6. Type the name of the user to be authorized in the text box and click **Check Names**. The following example shows selection of a group.



7. Click **OK**.

Add Users or Groups to HerculesDownloadServerUsers Local Group

Only Windows users that are members of the *HerculesDownloadlServerUsers* Local Group, that is, local to the Hercules Download Server, are given access to the Hercules Download Server web site.

Add Members to HerculesDownloadServerUsers in Windows 2000 Server

To add a user or group to the HerculesDownloadServerUsers Local Group

1. Log on to the server where the Hercules Download Server is installed.
2. From the **Start** menu, select **Settings > Control Panel**.
3. Select **Administrative Tools > Computer Management.**
4. Expand **Local Users and Groups** and click **Groups**.
5. Select **HerculesDownloadServerUsers**. Click Properties. Click **Add** to open Select Users, Computers, or Groups.
6. If needed, click **Locations**. Select the domain for the user or group to be authorized to configure the Hercules Channel Server. Click **OK**.
7. Type the name of the user or group to be authorized in the text box and click **Check Names**.
8. Click **OK** to close. Click **Apply** and then click **OK** to close HerculesDownloadServerUser Properties.

Add Members to HerculesDownloadServerUsers in Windows Server 2003

To add a user or group to the HerculesDownloadServerUsers Local Group

1. Log on to the server where the Hercules Download Server is installed.
2. From the **Start** menu, select **All Programs > Administrative Tools > Computer Management.**

3. Expand **Local Users and Groups** and click **Groups**.
4. Open **HerculesDownloadServerUsers**. Click **Add** to open Select Users, Computers, or Groups.
5. If needed, click **Locations**. Select the domain for the user or group to be authorized to configure the Hercules Channel Server. Click **OK**.
6. Type the name of the user or group to be authorized in the text box and click **Check Names**.
7. Click **OK**.

Set up Channel Server to Use SSL

SSL is a means by which the communication between point A and point B is secured from eavesdropping and tampering. Normally, SSL is used when the data being exchanged is sensitive, for example, Social Security numbers or financial data. It could be argued that the Hercules Channel Server data is sensitive: by looking at the patch requests from the Hercules Server to the Channel Server, a person could, theoretically, find out what vulnerabilities are being scheduled for remediation and then exploit these vulnerabilities before they are remediated. Even if the data were not deemed sensitive, you may, as a corporate policy, require secure communications in all cases.

Use the following procedure to set up the Channel Server to use SSL.

To set up the Channel Server to use SSL

1. Open Windows Explorer and navigate to:

   `C:\Program Files\Citadel\Hercules\Channel Server\Services`

2. Open the following file in an editor such as Notepad:

   `CitadelSecurity.Hercules.Channel.Service.exe.config`

3. At the same level as <runtime> under <configuration> add the following three lines, substituting `r09u24` with the host name or IP addrress of your Channel Server:

```
<appSettings>
    <add key="WebServiceUrl" value="https://r09u24/" />
  </appSettings>
```

4. Save the changes to the configuration file.

Complete Hercules Reporting Setup

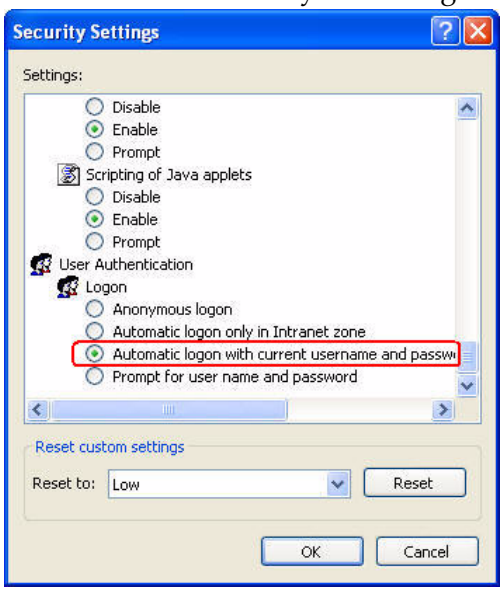
To generate Hercules Reports without supplying credentials each time, you can configure the Hercules Administrator to trust the Hercules Server.

To use login credentials for Hercules report generation

1. From the Start Menu, select **Control Panel > Internet Options**.

2. Tab to Security, click the **Trusted sites** icon, then click **Custom Level** to open Security Settings.

3. Scroll to the bottom of the Settings list box. Under User Authentication Logon, select **Automatic Logon with current username and password**. Then click **OK** to save your settings and close Security Settings.



4. Click **OK** to exit Internet Properties.

Create Accounts for Other Hercules Users

This section describes how to perform the following procedures:

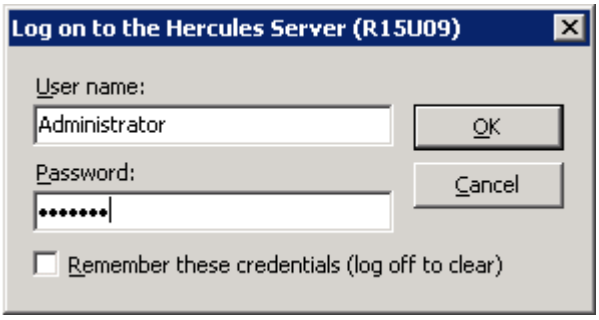
- "Add Administrator-Privileged Accounts for Managing Hercules Clients" (page 3-7)
- "Grant User Access to the Hercules Server and Assign Roles" (page 3-10)

Add Administrator-Privileged Accounts for Managing Hercules Clients

This section describes how to configure Client Management Service (CMS) in the Hercules Server and add the credentials needed to install the Hercules Client on the devices to be managed. CMS requires a domain administrator or administrator-privileged account. These credentials are also required to remediate devices from the Hercules Server. Entry of multiple credentials for administrator accounts in different domains enables clients in different domains to be managed from a singe Hercules Server.

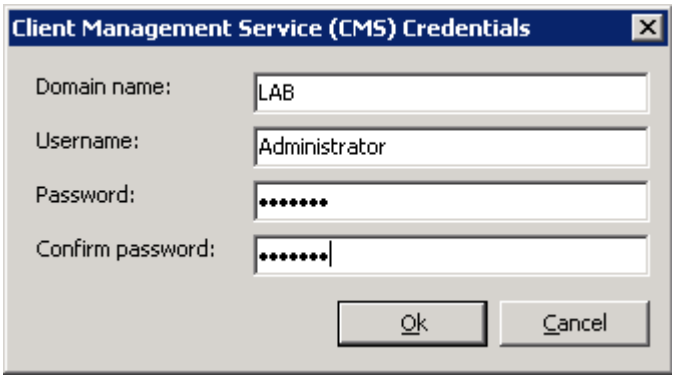
To add credentials required for Client Management Services (CMS)

1. Click the Windows **Start** button. From the Start menu, select **All Programs > Hercules > Hercules Administrator**.
2. If you did not select the option to remember your credentials, the Log on to the Hercules Server dialog displays. Type the name with which you logged into the server in the **User name** text box. Type the associated password in the **Password** text box. Then, click **OK** to log on.



3. From the Navigation pane, select **Hercules Servers** to open Manage Hercules Servers.
4. Right-click the Hercules Server and select **Properties.**

5. To manage client devices on a given Windows domain, do the following:
   a. Click **Add** to open Client Management Service (CSM) Credentials.



   b. Enter that domain name for **Domain name**. For **Username** and **Password**, enter administrator-privileged credentials for this domain or the credentials of the domain administrator. For **Confirm password**, retype the password. Click **OK** to add the account.
   c. Repeat the last two steps to add other CMS credentials for this domain or other domains.

   Tip: For Windows, the credentials you enter here must be defined under Computer Management > System Tools > Local Users and Groups > Groups > Administrators. That is, the credentials must be added to Administrators Properties. This dialog is accessed from the Start menu option, Administrative Tools.

6. To manage UNIX devices, verify that the User account is root or, if not, change it. Accept the default of **Remote root logon access**, if appropriate, or change it to **SUDO root access**.

   Important: For information on configuring SSH and generating an SSH public key for Hercules Clients installed on UNIX, Linux, and Mac OS X devices, see the *Hercules User's Guide* section under Manage Hercules Clients on configure Hercules clients to connect through CMS.

7. Click **OK**.

   Note: To use the command line alternative, enter the following from the server on which you installed the Hercules Server:

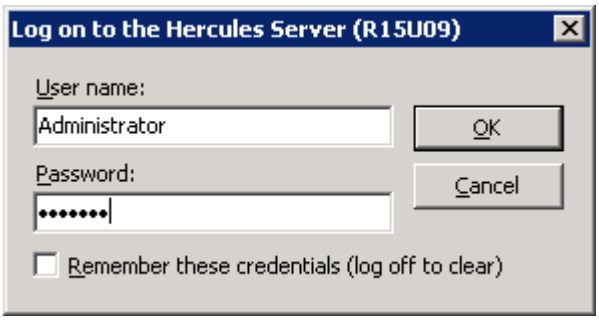
   ```
   C:\Program Files\Citadel\Hercules\Services\ClientMgrService -
   install
   ```

Grant User Access to the Hercules Server and Assign Roles

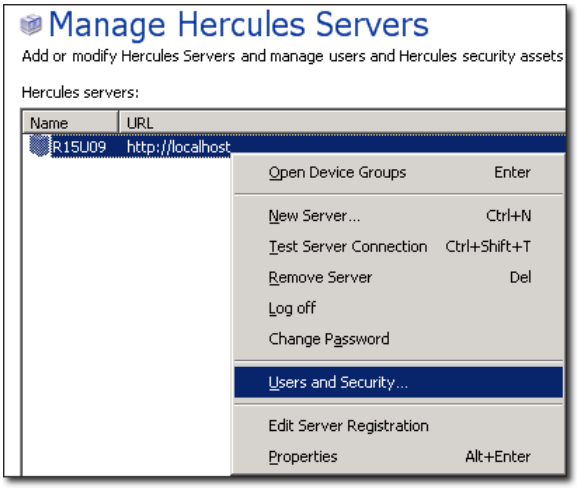
Only a Hercules user with the role of Hercules System Administrator is permitted to grant users access to the Hercules Server. At installation, you as the installer are automatically added as a user with the role of Hercules System Administrator. To assign the task of granting user access to someone else, you must grant that user access to the Hercules Server and assign the Hercules System Administrator role. See the *Hercules User's Guide* section, Configure Users and Security in the Hercules Server, for details.

To grant user access to the Hercules Server and assign roles

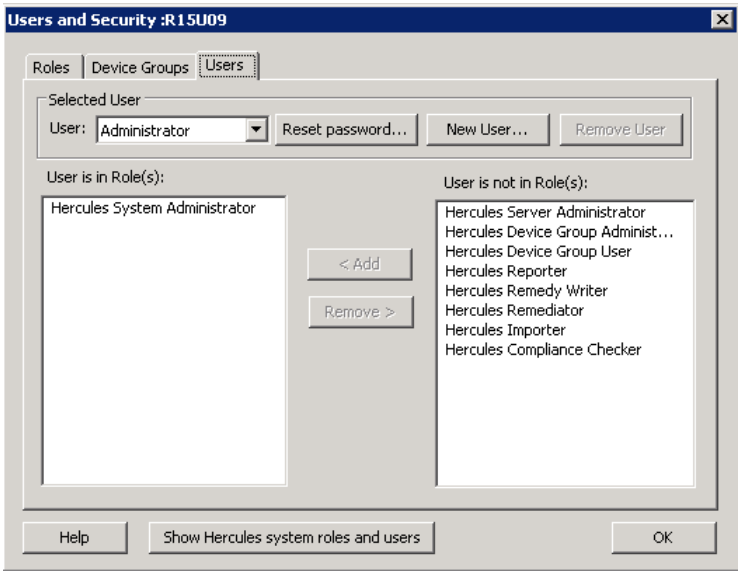
1. Click the Windows **Start** button. From the Start menu, select **All Programs > Hercules > Hercules Administrator**.
2. If you did not select the option to remember your credentials, the Log on to the Hercules Server dialog displays. Type the name with which you logged into the server in the **User name** text box. Type the associated password in the **Password** text box. Then, click **OK** to log on.



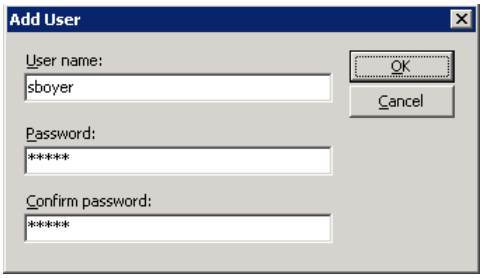
3. Click **Close** to close the Hercules QuickStart.
4. From the Navigation pane, select **Hercules Servers** to open Manage Hercules Servers.
5. Right-click the Hercules Server name you entered and select **Users and Security** to open Users and Security for this server.



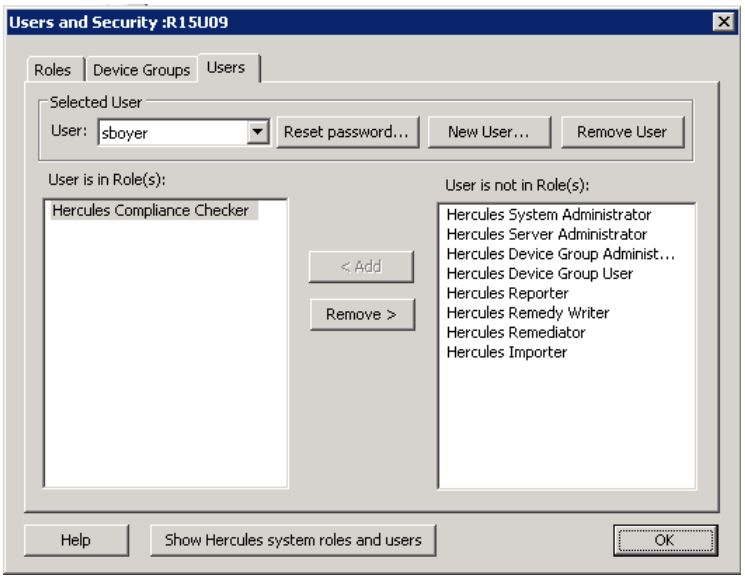
6. Select the Users tab. Notice that the user name with which you logged on was added as a Hercules user and appears as the Selected User with the role, Hercules System Administrator. This role is automatically assigned to the installer. Click the **New User** button to open the Add User dialog box.



7. Add the new user as follows:
   a. Type the name of the Hercules user in the **User name** text box.
   b. Type the Hercules password to assign to this user in the **Password** text box. (You can assign the same password to all users. Each user can reset that password to a unique password.)
   c. Retype the same password in the **Confirm password** text box.
   d. Click **OK**.



8. Under the **User is not in Role(s)** box, select a role for the user, and click **Add** to add the user name to **User is in Role(s)**. For a full description of each role, see the *Hercules User's Guide*.



9. Repeat Step 7 and Step 8 for all the users you want to allow to access this server. Then click **OK**.

   Note: The users you authorize can install the Hercules Administrator on their host machines, add this server by its IP address, and perform tasks permitted by the role you assigned.

Initialize V-Flash

Citadel V-Flash team members review new vulnerabilities as they are discovered and write and test remediations to address these vulnerabilities. The remediations are then made available through V-Flash for system administrators to update their Hercules Servers. New remediations are made available almost daily and an e-mail is also sent out informing users of a new update. Citadel provides the V-Flash server, which communicates directly over HTTPS with the V-Flash client located on your Hercules Server. You can manage your V-Flash downloads from the Hercules Administrator. User configuration includes: updating the V-Flash interval, monitoring V-Flash status, and configuring HTTPS.

V-Flash is not automatically initiated after installation. For details on initiating V-Flash, see the *Hercules Users Guide*.

4. Registration and Licensing

A *trial license key* enables you to use all features of the Hercules software for a limited period of time with a limited number of devices.

A *retail license key* enables you to use the selected set of Hercules features for all the devices you need to manage. You can install Hercules with a retail license without having used a trial license or you can try out Hercules with a trial license and then upgrade later to a retail license. Activation of a retail license requires Internet connectivity.

This chapter addresses the following:

For more information on licensing Hercules software, call Customer Support. For contact information, see "Customer Support" in the Before You Begin section of this manual.

Configure a Retail License

Hercules software is licensed based on the number of devices to be managed and the selected feature set. Hercules v4.0 comes with a set of core features. In addition, you can separately license other features. For a full description of core features and licensed features, see the first chapter of the *Hercules User's Guide*.

When you purchase the Hercules software, you get a license key. When you install the Hercules Server, you enter this key. Once you begin using the Hercules Server, it checks in daily with the Citadel back office. The back office software ensures you get full usage of the features you purchased for the device count you specified. If you decide at any time to license additional features, just call Customer Support with your request. The next time your Hercules server checks in, your additional features will be enabled. Customer Support may suggest that you take action to force *immediate* registration of your new Hercules system.

Use the following procedure described in this section in the following cases:

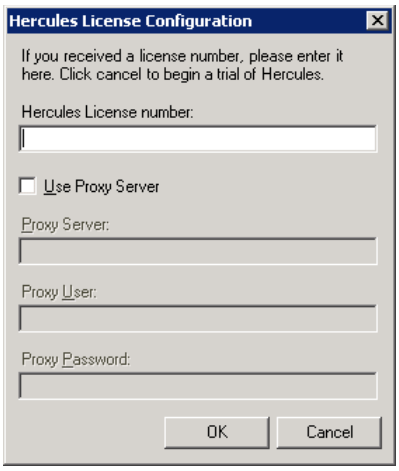
- To force immediate registration of a newly installed Hercules system
- To enable additional separately-licensed features
- To upgrade from a trial license to a retail license without reinstalling the Hercules system

To configure a retail license

1. From Windows Explorer on the server where you installed the Hercules Server, navigate to the following application (or browse to it from the Run dialog).

   ```
   C:\Program Files\Citadel\Hercules\Server\LicenseConfig.exe
   ```

2. Double click `LicenseConfig.exe` to open the following dialog box:



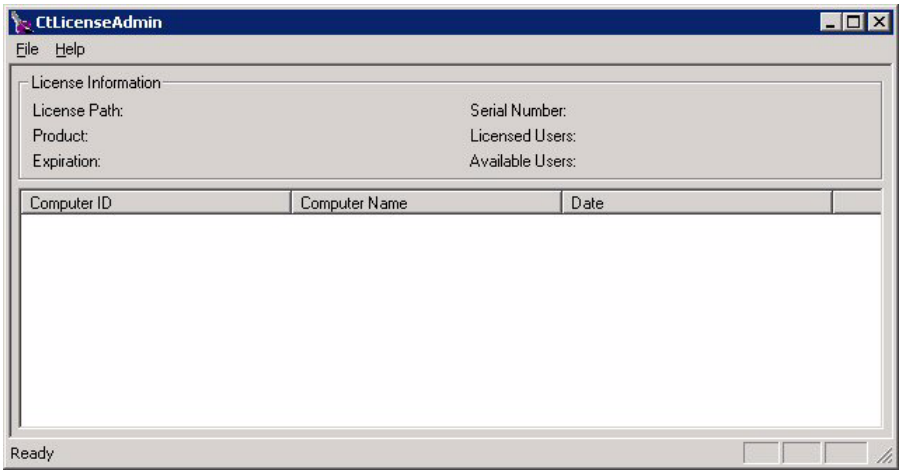
3. Type your license number in the Hercules License number field.
4. If you use a proxy server, check the Use Proxy Server checkbox, enter the proxy server name, proxy userid, and proxy password.
5. Click **OK** to send your key to the Citadel back office, which registers your Hercules software and activates the features you have purchased for the device count you established.

Extend a Trial License

You may have installed the Hercules system with a trial license. A trial license enables you to use all Hercules features to manage and remediate ten devices for 30 days from the time of installation. To obtain authorization to use the Hercules system with more than ten devices or to extend the trial period, use the following procedure.

To extend the trial license for Hercules software

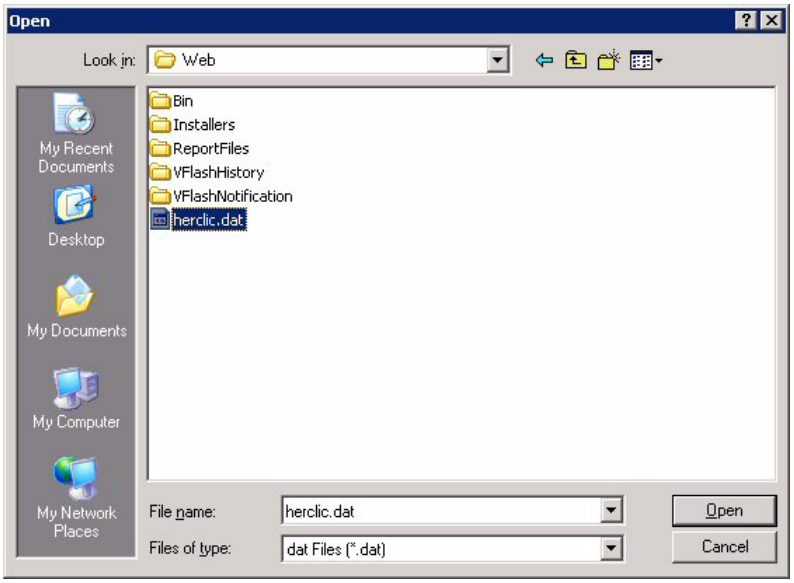
1. Log onto the server where you have installed the Hercules server. Click the Windows **Start** button, select **All Programs >Hercules > LicenseAdmin**.



2. From the File menu, select **Open**. Navigate to the following folder:

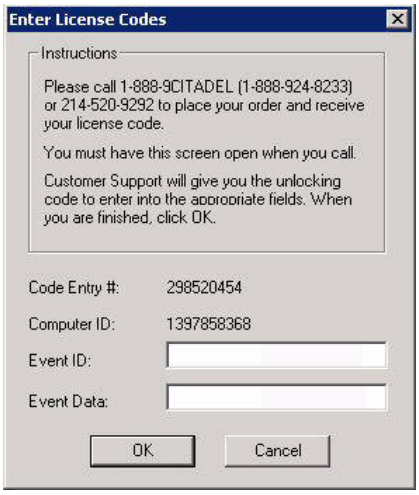
   `C:\Program Files\Citadel\Hercules\Server\Web\HerculesSErver`

3. Select the file, **`herclic.dat`**, and click **Open**.

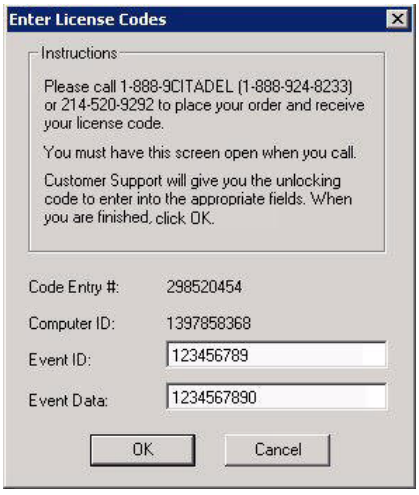


4. Notice that the licensing information is displayed.

5. From the File menu, select **Enter License Codes.**



6. While this dialog box is open, following the instructions for contacting Customer Support. Provide Customer Support with your Code Entry number and Computer ID.
7. Enter the data supplied by Customer Support for **Event ID** and **Event data**.



8. Click **OK** when the confirmation message displays.

9. Select **Exit** from the File menu.

5. Migrating from a Previous Version

The Hercules 4.0.x Data Migration Tool enables you to migrate data from an existing Hercules 3.5.1 system to a newly installed Hercules 4.0.x system.

After migration, your previous definitions of Hercules users and their assigned roles and all of your customized policies will be part of your new installation. This process also migrates the following data: vulnerabilities, devices, device groups, device queries, imports, scheduled remediations, and profiles. You can use this tool to migrate the data in the main Hercules database and/or the user-modified data in the Patch Manifest databases.

This chapter includes the following sections:

The procedures documented in this chapter assume you are migrating data from a 3.5.1 Hercules system with a single Hercules server to a 4.0 Hercules system with a single Hercules server. This could be either a standalone installation, where all Hercules servers are installed on the same system, or a distributed installation with a single Hercules server and multiple Hercules Download Servers. If you have multiple Hercules servers in your system, you will perform the migration of the Hercules database for each 3.5.1-to-4.0 pair. If your system is distributed such that the Hercules Channel Server is on a different machine than the Hercules Server, you will perform the v3.5.1 backup of the Hercules Patch Manifest database and the subsequent v4.0 migration from the servers where the Channel Server for each release is installed.

Migration Approaches

This section describes the steps to follow for each of the following three migration approaches:

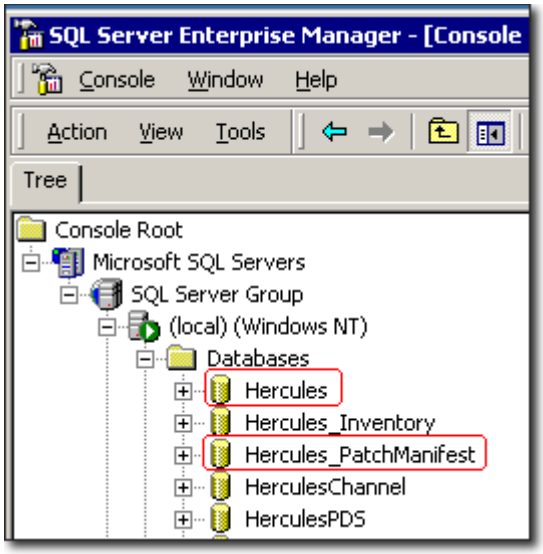
The recommended approach for upgrading to Hercules v4.0 is to leave your v3.5.1 Hercules server active while you install the Hercules v4.0 server on a different machine. After you are comfortable with the new Hercules v4.0 functionality, you back up your v3.5.1 data and use the Hercules Data Migration tool to migrate your pre-v4.0 data to the Hercules databases on the SQL server you selected for v4.0. The migration process allows you to port your v3.5.1 configuration information to the v4.0 version of Hercules, whether you are using a Hercules appliance or have installed Hercules v4.0 on an existing server.

However, you may wish to install v4.0 on the same server where you previously installed v3.5.1 and still migrate your data. This scenario is supported.

Migrating a v3.5.1 Source Database to a v4.0 Destination System

Migration from one database to the other is the preferred method when the v3.5.1 Hercules system and the v4.0 Hercules system are operating in parallel. When migrating directly from an existing installation, you supply the connection string to the database so that migration can begin.

Two databases can be migrated: the Hercules database and the Hercules_PatchManifest database.



To migrate from a v3.5.1 system on one server to a v4.0 system on another server

1. Continue using your v3.5.1 Hercules system.
2. Prepare to install v4.0 on a different server than where your v3.5.1 system is running. Complete any preparation steps that you may have previously not performed. For example, see "SQL Server and Reporting Services Setup" on page 1-17.
3. Install the Hercules v4.0 system. See Chapter 2, "Installing Servers and Administrator" on page 2-1.
4. Review "Completing Post Installation Setup" on page 3-1 for any tasks that you need to perform for v4.0. For example, "Complete Hercules Reporting Setup" on page 3-6.
5. Become familiar with the new v4.0 functionality
6. Log on to the Hercules v3.5.1 server and prepare for migration as follows:
   - Back up all of the Hercules v3.5.1 databases.
   - "Review Windows and Unix Accounts for Possible Export"
   - "Install Hercules Credential Exporter"
   - "Export Windows and Unix Credentials to a Local Text File"
   - Make a system image backup with a tool such as Ghost.
7. Log on to the Hercules 4.0 server and prepare for migration as follows.
   - "Run V-Flash Now on the Hercules v4.0 Server"
   - "Ensure Access to the Source Database or Data Files"
   - "Install the Hercules Data Migration Tool"
8. From the server with the v4.0 Hercules Server, use the Migration Tool to connect to the existing 3.5.1 Hercules server source database and migrate user information, vulnerabilities, devices and device groups, policy information, device queries, imports, scheduled remediations and profiles. For details, see "Migrate the Hercules Database, Data File or Backup File" on page 5-19.
9. From the server with the v4.0 Hercules Channel Server, use the Migration Tool to connect to the 3.5.1 Patch Manifest database and migrate the patch download URL information as well as the install and compliance scripts. For details, see "Migrate the Hercules Patch Manifest Database, Data File or Backup File" on page 5-35.
10. Ensure Hercules clients from v3.5.1 check in to the new v4.0 server. See "Ensure v3.5.1 Clients Update to v4.0 and Check in with v4.0 Servers" on page 5-45.
11. Uninstall Hercules v3.5.1 as described in "Removing Software Permanently" on page A-1.

Migrating a v3.5.1 Source Backup File (.bak) to a v4.0 Destination System

Migration from a backup file can be used when migrating inplace, where you install Hercules 4.0 on the same system that Hercules 3.5.1 was installed on.

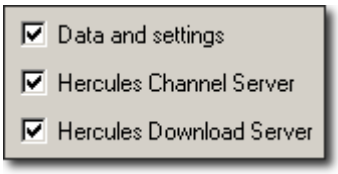
Before migrating from *.bak files, back up the databases using your standard, local procedure.

During migration, the Hercules Data Migration Tool restores the database from the backup file (.bak) using a process similar to the attach process.

Note Please contact Citadel Security Software Customer Support for guidance.

To migrate from 3.5.1 backup files to a v4.0 system on the same server

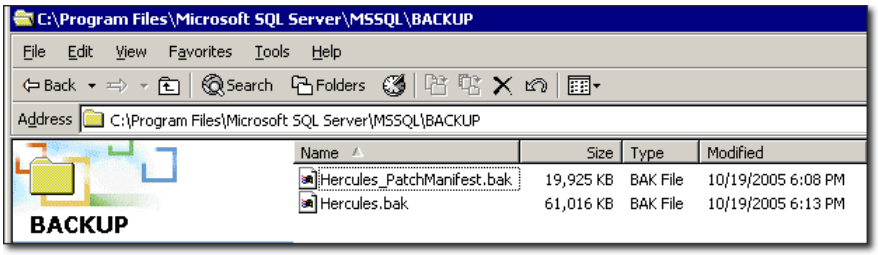
1. Log on to the server where the 3.5.1 Hercules standalone system is installed.
2. Use your local backup procedures to back up the Hercules database and the Hercules Patch Manifest database. If using SQL Enterprise Manager, the default path is `C:\Program Files\Microsoft SQL Server\MSSQL\BACKUP\`.
3. Make a system image backup with a tool such as Ghost.
4. Optionally, prepare to migrate CMS credentials as follows:
   - "Review Windows and Unix Accounts for Possible Export" (page 5-8)
   - "Install Hercules Credential Exporter" (page 5-9)
   - "Export Windows and Unix Credentials to a Local Text File" (page 5-13)
5. Uninstall Hercules v3.5.1 as described in "Removing Software Permanently" on page A-1. When presented with options to uninstall, check all three options.



6. Prepare to install v4.0, completing any preparation steps that you may have previously not performed. For example, see "SQL Server and Reporting Services Setup" on page 1-17.
7. Install Hercules v4.0 on that same system. See "Install v4.0 Servers in a Standalone Architecture" on page 2-2.
8. Install the Administrator. See "Install the Hercules Administrator" on page 2-27.
9. Review "Completing Post Installation Setup" on page 3-1 for any tasks that you need to perform for v4.0. For example, "Complete Hercules Reporting Setup" on page 3-6
10. Verify your access as described in "Ensure Access to the Source Database or Data Files" on page 5-14.

11. Install the migration software as described in "Install the Hercules Data Migration Tool" on page 5-15.
12. Run V-Flash Now. For instructions, see "Run V-Flash Now on the Hercules v4.0 Server" on page 5-14.
13. Prevent devices from checking in until data migration completes as follows:
    a. Log on to the v4.0 Administrative console.
    b. In the Navigation bar under Device, click **Device Groups**.
    c. If the Default Group is displayed with more than 0 devices, double-click Default Group to open Manage Devices, which displays the 3.5.1 devices that have already installed themselves.
    d. Select all the displayed devices and click **Remove**.
    e. Click **Yes** to the confirm removal of the selected devices.
    f. Exit the Hercules Administrator
    g. Display the command prompt. (From the Start menu, select Command Prompt.)
    h. Type **`IISRESET /stop`** to temporarily stop IIS and prevent devices from checkin in until the data has been migrated.
14. Migrate user information, vulnerabilities, devices and device groups, policy information, device queries, imports, scheduled remediations and profiles from the `hercules.bak` file as described in "Migrate the Hercules Database, Data File or Backup File" on page 5-19.

    The backup files used in this chapter were created with the Backup Database option of the SQL Server Enterprise Manager. The backup files are called `Hercules.bak` and `Hercules_PatchManifest.bak`, but your files could have other names. The example backups were saved to the default destination path: `C:\Program Files\Microsoft SQL Server\MSSQL\BACKUP`.



15. Migrate the patch download URL information as well as the install and compliance scripts from the `PatchManifest.bak` file as described in "Migrate the Hercules Patch Manifest Database, Data File or Backup File" on page 5-35.
16. From a command prompt, type **`IISRESET /start`** to restart IIS. This enables Hercules Clients to check in with the new v4.0 Hercules server in the Device Groups migrated from the source 3.5.1 system.

Migrating a v3.5.1 Source Database File (.mdf) to a v4.0 Destination System

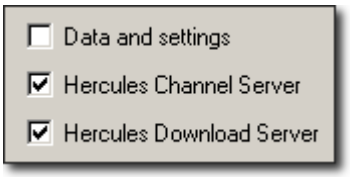
Migration from a detached database file can be used when migrating inplace, where you install Hercules 4.0 on the same system that Hercules 3.5.1 was installed on.

Note Please contact Citadel Security Software Customer Support for guidance.

If migrating from a detached database, that database must be attached and running before the migration can occur. In this case, you browse to the .mdf file and the migration tool reattaches the database and begins the migration.

To migrate from 3.5.1 Master Database files (.mdf) to v4.0 system on same server

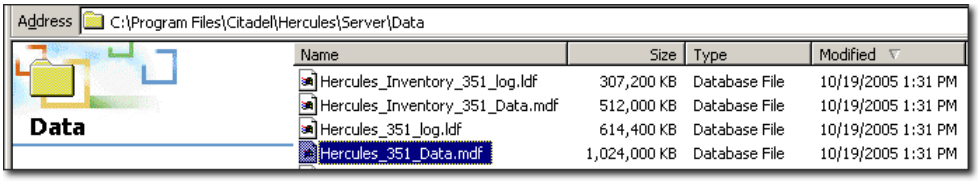
1. Log on to the server where the 3.5.1 Hercules standalone system is installed.
2. Make a system image backup with a tool such as Ghost.
3. Optionally, prepare to migrate CMS credentials as follows:
   - "Review Windows and Unix Accounts for Possible Export" (page 5-8)
   - "Install Hercules Credential Exporter" (page 5-9)
   - "Export Windows and Unix Credentials to a Local Text File" (page 5-13)
4. Uninstall Hercules v3.5.1 as described in "Removing Software Permanently" on page A-1. When presented with options to uninstall leave Data and settings unchecked.



Note -The Uninstall process detaches the v3.5.1 Hercules database and the 3.5.1 Hercules Patch Manifest database and leaves the source database files at their existing location. By default the location of the `Hercules_351_Data.mdf` file is `C:\Program Files\Citadel\Hercules\Server\Data`. The location of the `Hercules_PatchManifest_351.mdf` file is `C:\Program Files\Citadel\Hercules\Server\Channel Server\Data`

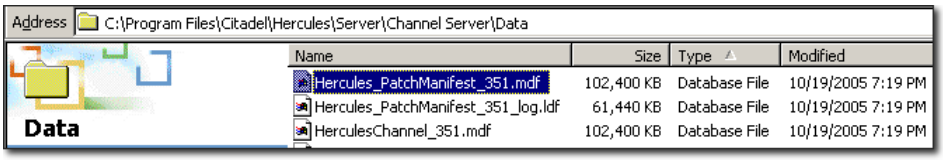
5. Prepare to install v4.0, completing any preparation steps that you may have previously not performed. For example, see "SQL Server and Reporting Services Setup" on page 1-17.
6. Install Hercules v4.0 on that same system. See "Install v4.0 Servers in a Standalone Architecture" on page 2-2.
7. Review "Completing Post Installation Setup" on page 3-1 for any tasks that you need to perform for v4.0. For example, "Complete Hercules Reporting Setup" on page 3-6.
8. Install the Administrator. See "Install the Hercules Administrator" on page 2-27.

9. Prevent devices from checking in until data migration completes as follows:
   a. Log on to the v4.0 Administrative console.
   b. In the Navigation bar under Device, click **Device Groups**.
   c. If the Default Group is displayed with more than 0 devices, double-click Default Group to open Manage Devices, which displays the 3.5.1 devices that have already installed themselves.
   d. Select all the displayed devices and click **Remove**.
   e. Click **Yes** to the confirm removal of the selected devices.
   f. Exit the Hercules Administrator.
10. From the command prompt, type **`IISRESET /stop`** to temporarily stop IIS and prevent devices from checkin in until the data has been migrated.
11. Migrate user information, vulnerabilities, devices and device groups, policy information, device queries, imports, scheduled remediations and profiles from the `Hercules_351_Data.mdf` file as described in "Migrate the Hercules Database, Data File or Backup File" on page 5-19. The example path of the `Hercules_351_Data.mdf` file follows:
    `C:\Program Files\Citadel\Hercules\Server\Data`



Note The Hercules Data Migration Tool reattaches the v3.5.1 Hercules database.

12. Migrate the patch download URL information as well as the install and compliance scripts from the `Hercules_PatchManifest_351.mdf` file as described in "Migrate the Hercules Patch Manifest Database, Data File or Backup File" on page 5-35.The example path of the `Hercules_PatchManifest_351.mdf` file follows: `C:\Program Files\Citadel\Hercules\Server\Data`



Note The Hercules Data Migration Tool reattaches the v3.5.1 Hercules Patch Manifest database.

13. From a command prompt, type **`IISRESET /start`** to restart IIS. This enables Hercules Clients to check in with the new v4.0 Hercules server in the Device Groups migrated from the source 3.5.1 system.

Prepare for Data Migration

This section includes procedures you perform on both the v3.5.1 source server and the v4.0 destination server. These may be different servers or the same server. For suggestions of when to perform these tasks, see the task flow corresponding to your migration approach under "Migration Approaches" on page 5-1.

On the Hercules v3.5.1 server:

- "Review Windows and Unix Accounts for Possible Export"
- "Install Hercules Credential Exporter" (page 5-9)
- "Export Windows and Unix Credentials to a Local Text File" (page 5-13)
- Make a system image backup with a tool such as Ghost.

On the Hercules v4.0 server:

- "Run V-Flash Now on the Hercules v4.0 Server" (page 5-14)
- "Ensure Access to the Source Database or Data Files" (page 5-14)
- "Install the Hercules Data Migration Tool" (page 5-15)

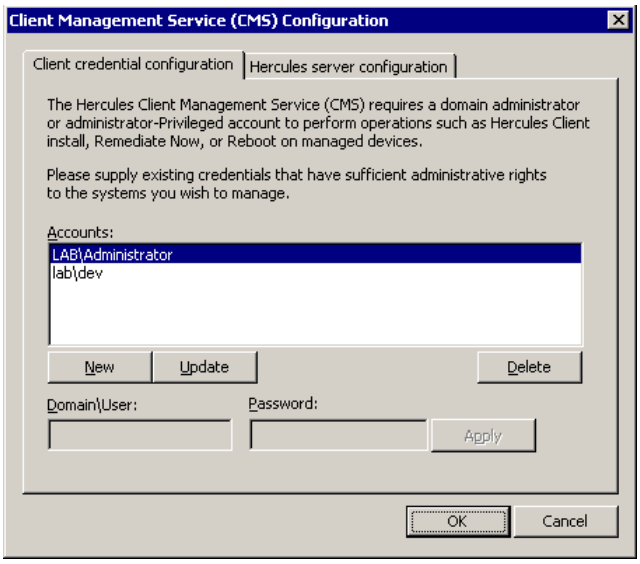
Review Windows and Unix Accounts for Possible Export

Before you install the Hercules Credential Exporter, review the credentials you have configured and determine whether to export them.

To review your current CMS credential settings

1. Log on to the server where the Hercules v3.5.1 server is running.
2. From the Start menu, select **Run**. Type **`cmd`** and click **OK**.
3. Type **cd ** to display the root directory.dir
4. Type: **cd `Program Files\Citadel\Hercules\Server\Services`** and press **Enter**.

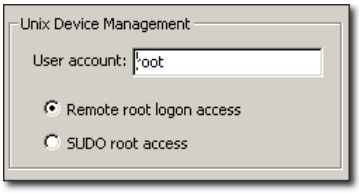
5. Type: **`ClientMgrService -install`** and press **Enter** to open the following dialog. Review the listed Accounts.



6. To export the listed accounts, create the Credential Exporter and then run it to begin the export.

To review the UNIX credential settings

1. From the Navigation pane, select Hercules Server.
2. Right-click a server and select Properties.
3. Select the Server Preferences tab.



4. To export the listed account, create the Credential Exporter and run it begin the export.

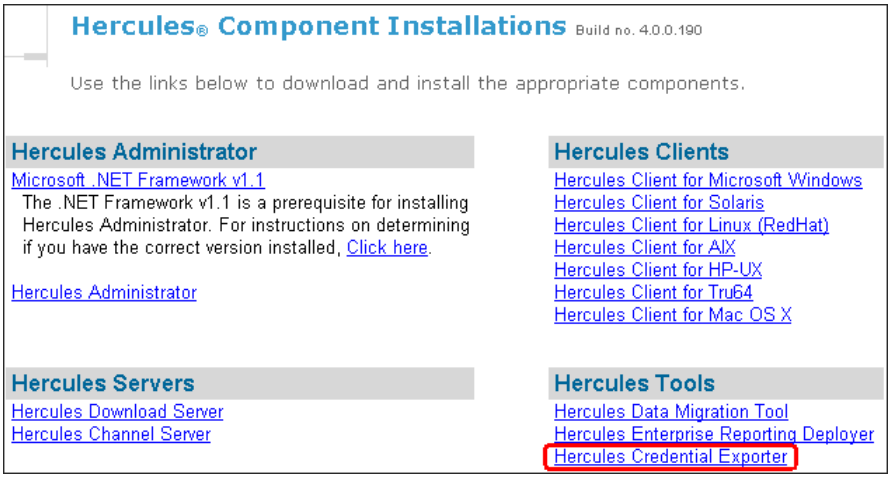
Install Hercules Credential Exporter

The Hercules Credential Exporter enables you to export all configured CMS credentials to a text file that will be moved to the new v4.0 installation when you run the Hercules Migration Tool.

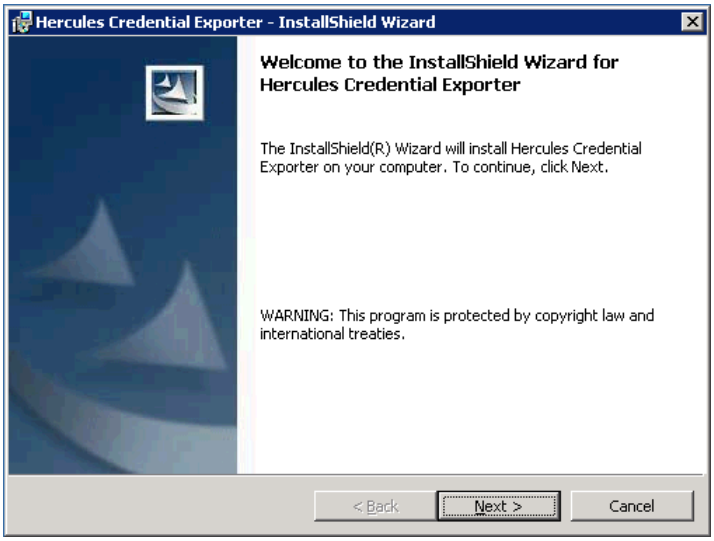
To create the Credential Exporter to export CMS and UNIX credentials

1. Log on to the server where the Hercules v3.5.1 server is installed.
2. Open Internet Explorer and enter the following in the Address bar:

   `http://<IP address of v4.0 server>/HerculesServer`

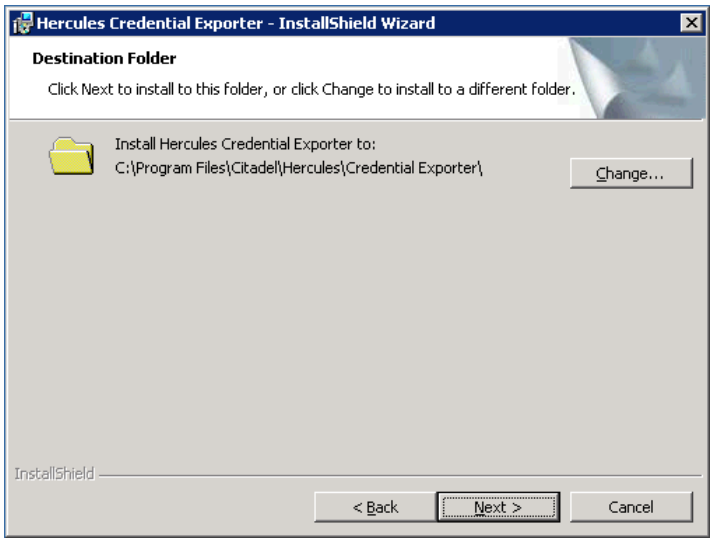


3. Click **Hercules Credential Exporter** and click Open to start the file download process. This opens the Welcome page of the Hercules Credential Exporter installer.

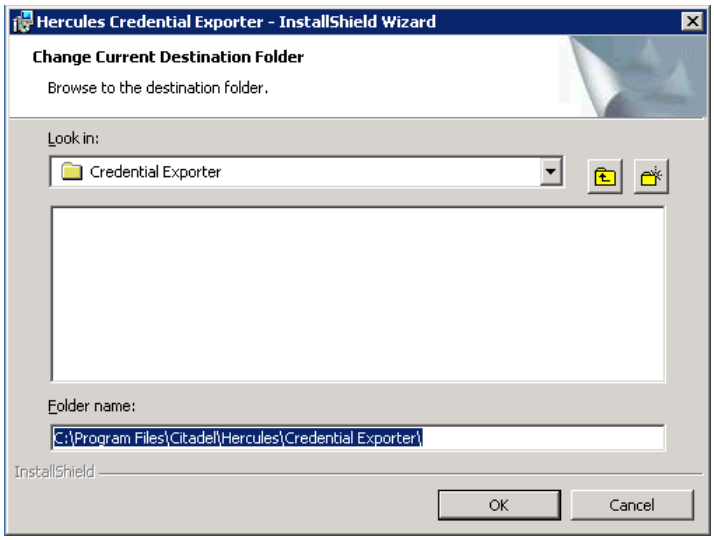


4. Click **Next** to open the Destination Folder page. Do one of the following:
   - To accept the default destination click **Next** and continue with Step 6.

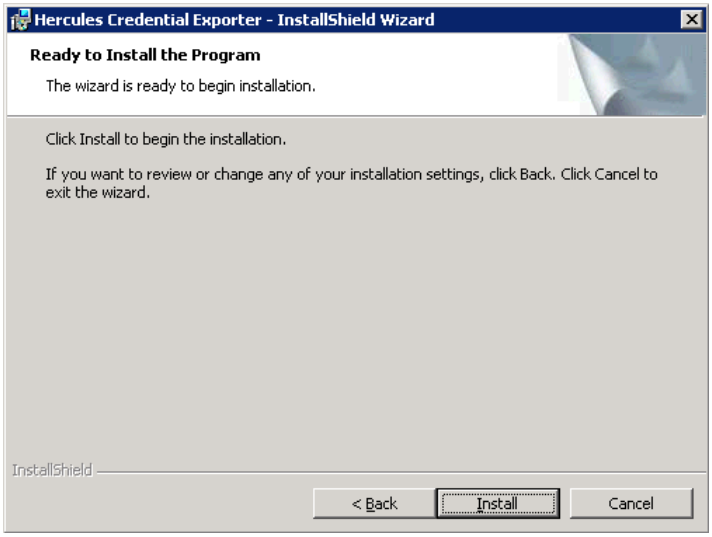
- To change the destination folder, click **Change** and continue with the next step.



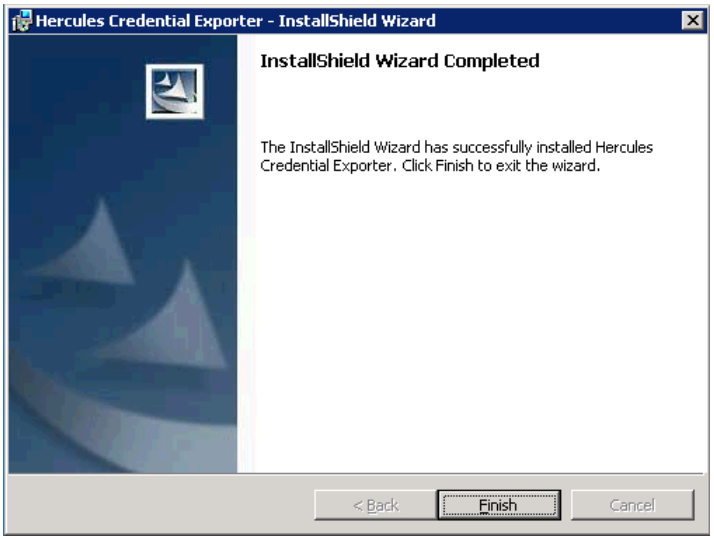
5. To change the destination folder, click **Change** to open the Change Current Destination Folder page. Browse to the desired destination folder, then click **OK**.



6. Click **Install** to begin the installation. The processing status displays momentarily.



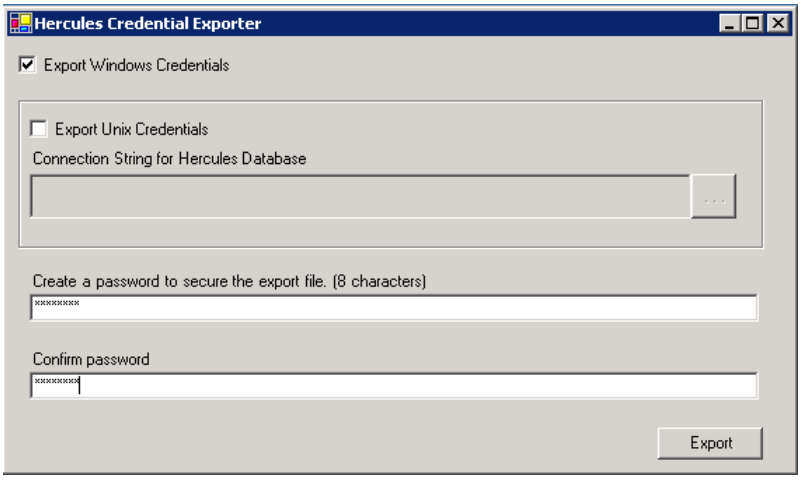
7. Click **Finish** to complete the installation of the Hercules Credential Exporter and exit the wizard.



Export Windows and Unix Credentials to a Local Text File

To run the Hercules Credential Exporter

1. Log on to the server where the Hercules v3.5.1 server is running.
2. From the **Start** menu, select **Programs > Hercules > Hercules Credential Exporter** to open the Hercules Credential Exporter.



3. Do one or both of the following:
   - To export CMS account credentials, select **Export Windows Credentials**.
   - To export UNIX credentials, select **Export Unix Credentials**. Then click the Browse button to select a connection string for the Hercules database.
4. For **Create a password to secure the export file**, type a password of at least 8 characters.
5. For **Confirm password**, retype the same password.
6. Click **Export**. The Save As window displays.

7. Save the file containing credentials to be exported as follows:
   a. Navigate to a location of your choice.
   b. For **Filename**, enter a name of your choice.
   c. Click **Save**. A confirmation message displays.

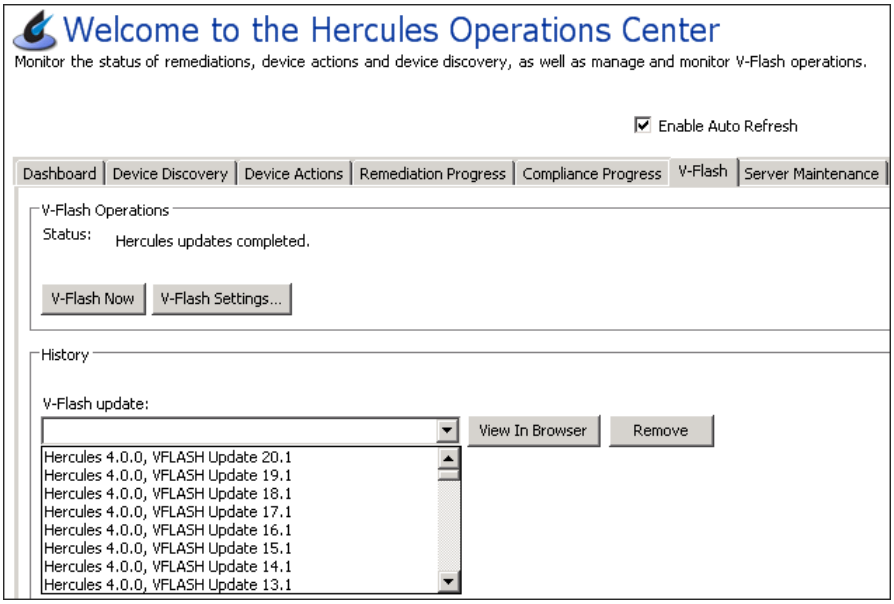
8. Click **OK**.

Run V-Flash Now on the Hercules v4.0 Server

To ensure data integrity, the destination server must be fully V-Flashed.

To ensure v4.0 Hercules server has all V-Flash updates

1. Open the v4.0 Hercules Administrator that is connected to the destination Hercules v4.0 server.
2. From the Operations Center V-Flash tab, click **V-Flash Now**.
3. Wait until the V-Flash Operations Status displays *Hercules updates completed.*



Ensure Access to the Source Database or Data Files

Ensure that you meet the following prerequisites to migration:

- The user who runs the Hercules Data Migration Tool must have administrative access to the Hercules SQL v4.0 database.
- The Hercules Data Migration Tool can access the 4.0 SQL database and the 3.5.1 database or data files.

If you, the logged on user, have administrative rights to an SQL or MSDE database, the Data Migration Tool will be able to access it. If the same logon is used to save the files as to run the Hercules Data Migration Tool, there will be no problem with the application accessing the files.

If migrating from a *.bak file, that file has to be on the same machine as the SQL server. Migrating from a *.bak file is used after uninstalling the 3.5.1 Hercules software and installing the 4.0 Hercules software on the same machine.

Install the Hercules Data Migration Tool

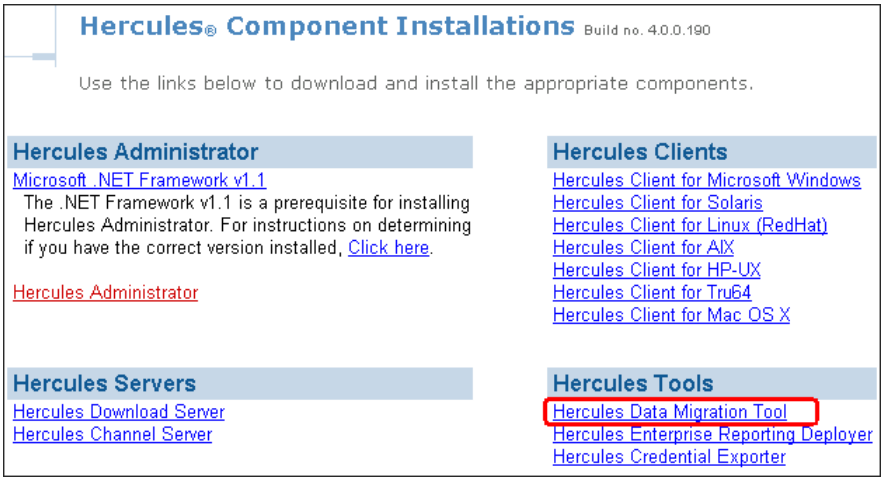
The Hercules Data Migration Tool is used on the machine that is the destination of the migration.

To install the Hercules Data Migration Tool

1. Log on to the server where the v4.0 Hercules server is installed.
2. From the **Start** menu, select **All Programs > Hercules > Hercules Installers**.

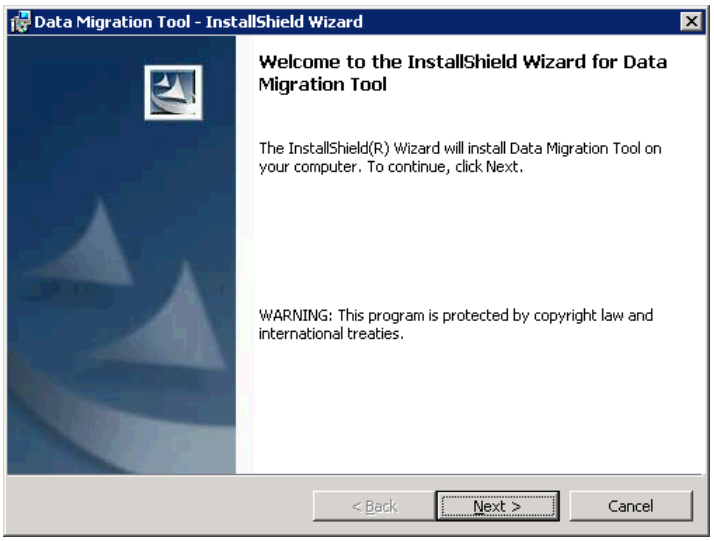
   Alternatively, open Internet Explorer and in the Address textbox enter the following to open Hercules Component Installations:

   ```
   http://<server hostname or IP address>/HerculesServer
   ```

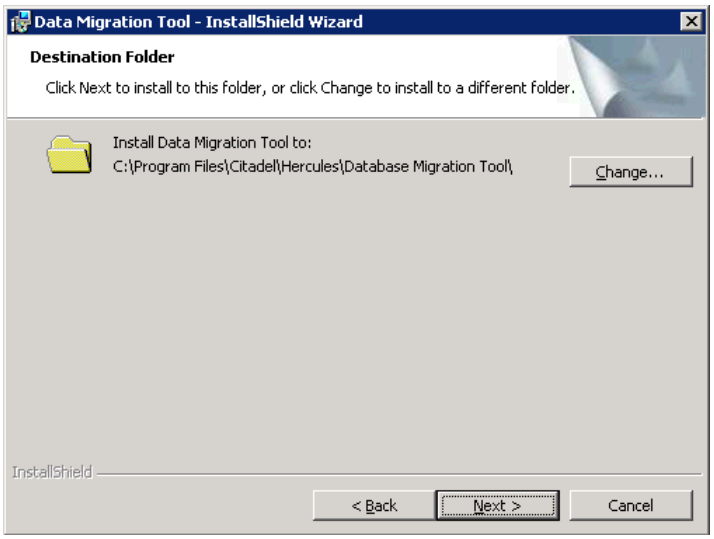


3. Under Hercules Tools, click **Hercules Data Migration Tool** to open the File Download dialog for DataMigration.exe.
4. Click **Open**.

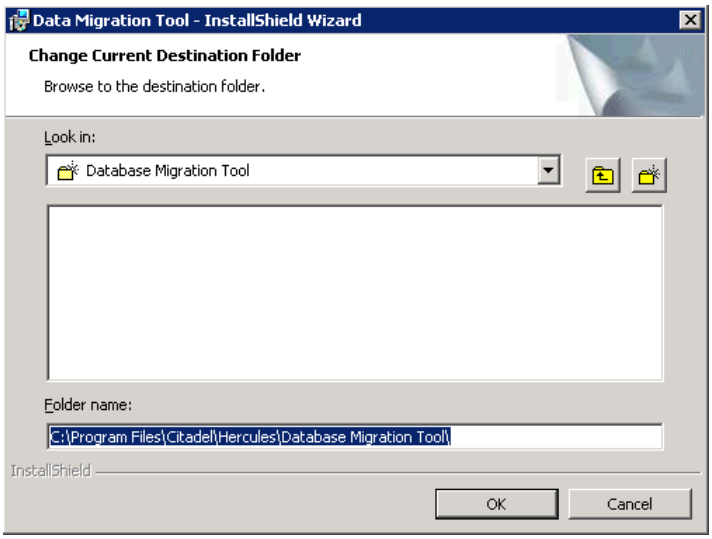
5. The Preparing to Install wizard displays momentarily, then the Welcome page of the wizard displays.



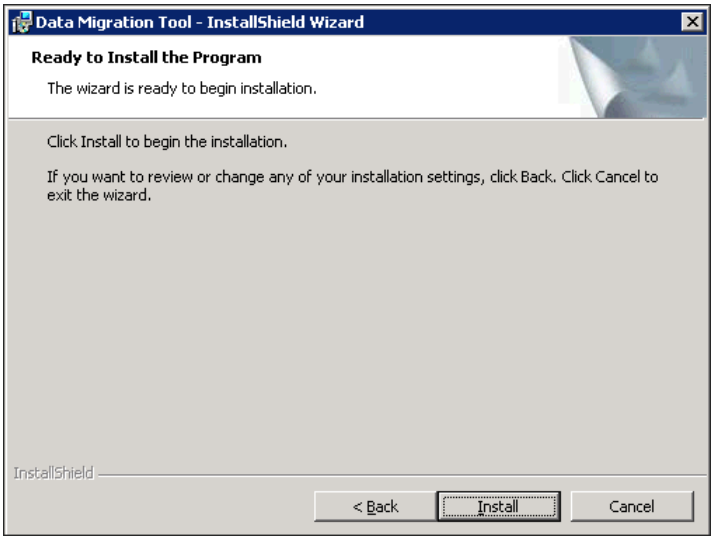
6. Click **Next** to open Destination Folder page. Do one of the following:
   - To accept the default destination, go to Step 8.
   - To change the destination folder, continue.



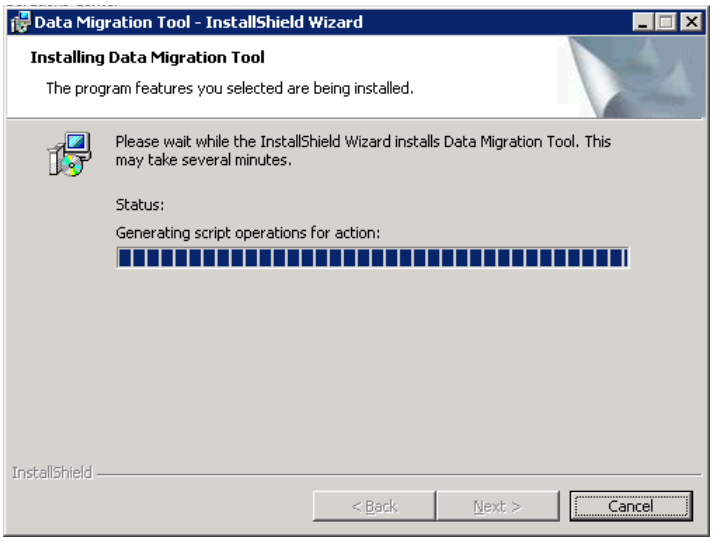
7. Click **Change** to open the Change Current Destination Folder page. Browse to the desired destination folder, then click **OK**.



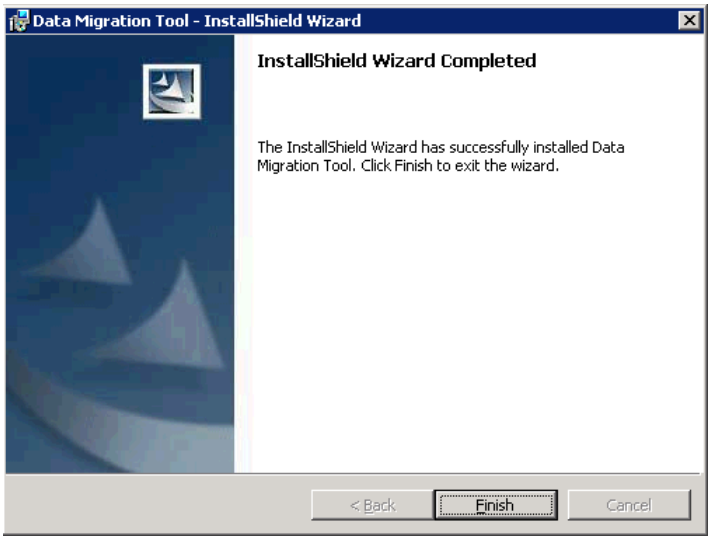
8. Click **Next** to open Read to Install the Program.



9. Click **Install** to begin the installation of the Data Migration Tool.



10. Wait while the processing completes. The Wizard Completed displays.



11. Click **Finish**.

Important - If your v4.0 destination system is distributed such that the Hercules Channel Server is on a different machine than the Hercules Server, repeat this procedure to install the Hercules Data Migration Tool on the server where the Hercules Channel Server is installed.

Migrate Data and Settings from Hercules v3.5.1 to Hercules v4.0

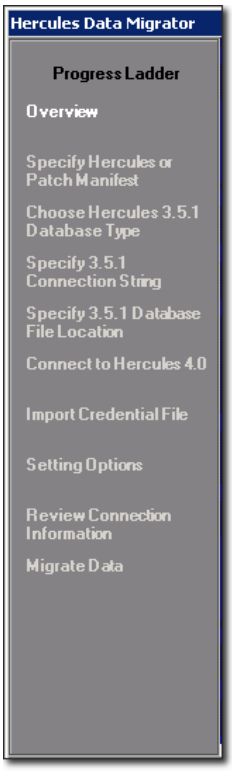
This section describes the following procedures:

- "Migrate the Hercules Database, Data File or Backup File"
- "Migrate the Hercules Patch Manifest Database, Data File or Backup File"

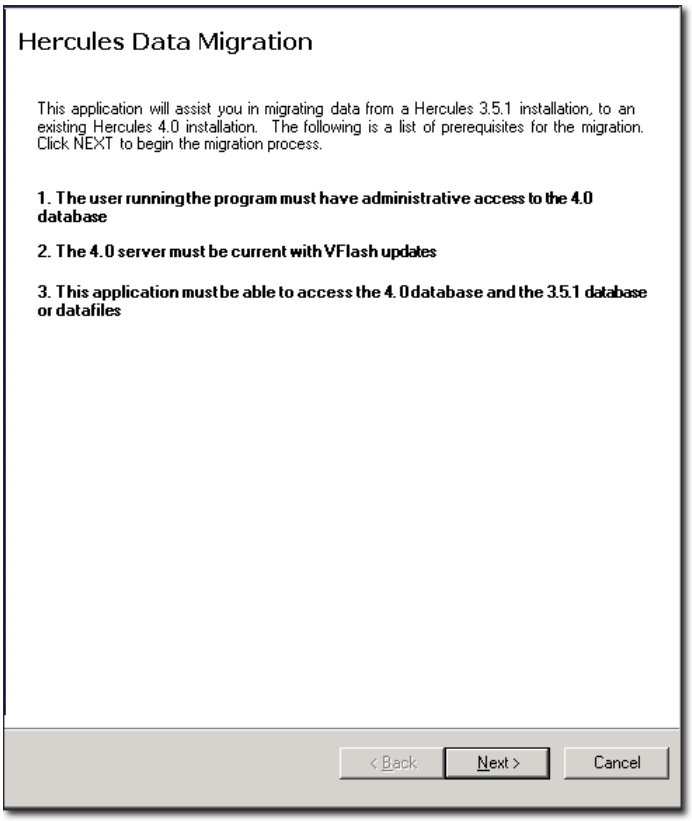
Migrate the Hercules Database, Data File or Backup File

To use the Hercules Data Migrator to migrate the Hercules database

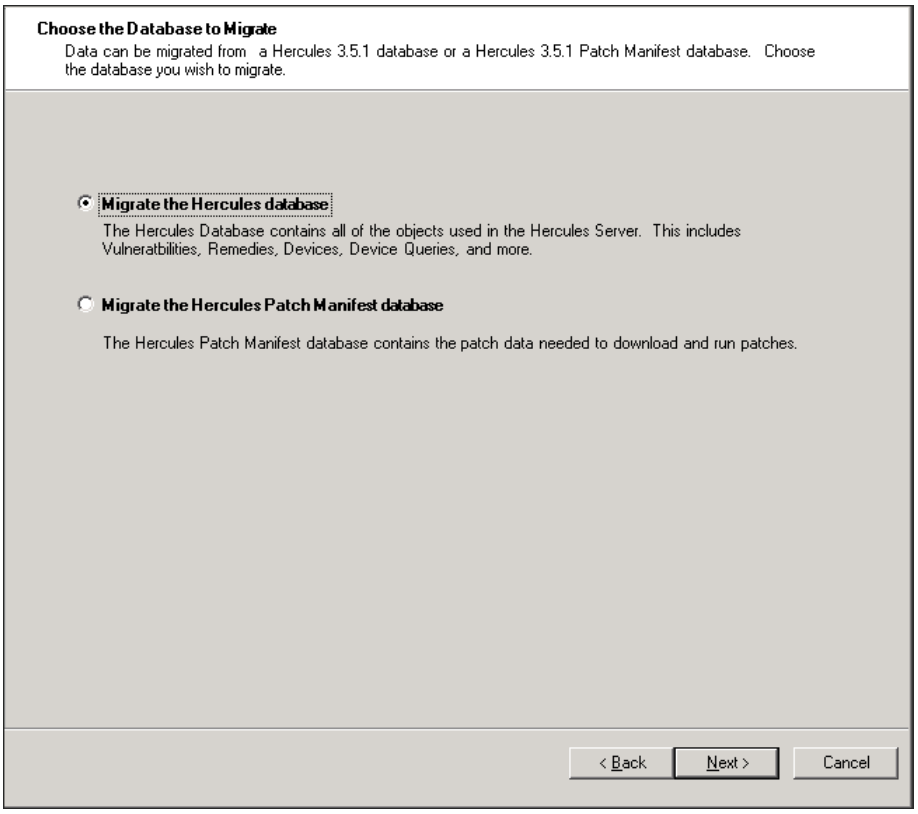
1. Complete the preceding steps in the workflow for your migration strategy.
   - If migrating the Hercules database, first complete Step 1 through Step 7 in "Migrating a v3.5.1 Source Database to a v4.0 Destination System" on page 5-3.
   - If migrating from a Hercules backup file, complete Step 1 through Step 13 in "Migrating a v3.5.1 Source Backup File (.bak) to a v4.0 Destination System" on page 5-5.
   - If migrating from a Hercules data file, complete Step 1 through Step 9 in "Migrating a v3.5.1 Source Database File (.mdf) to a v4.0 Destination System" on page 5-7.
2. Log on to the server where Hercules v4.0 is installed.
3. From the **Start** menu, select **All Programs > Hercules > Database Migration Tool**. The first page of the Hercules Data Migration tool displays. Notice the Progress Ladder. This gives you an overview of the steps for data migration. The step you are on is highlighted.



4. Ensure you have met the following prerequisites.
   - The credentials you used to log on with have administrative access to both the v3.5.1 and the v4.0 database.
   - The v4.0 server has been updated with the latest V-Flash updates.
   - This application can access both the Hercules v4.0 database and the Hercules v3.5.1 database (on separate machines).

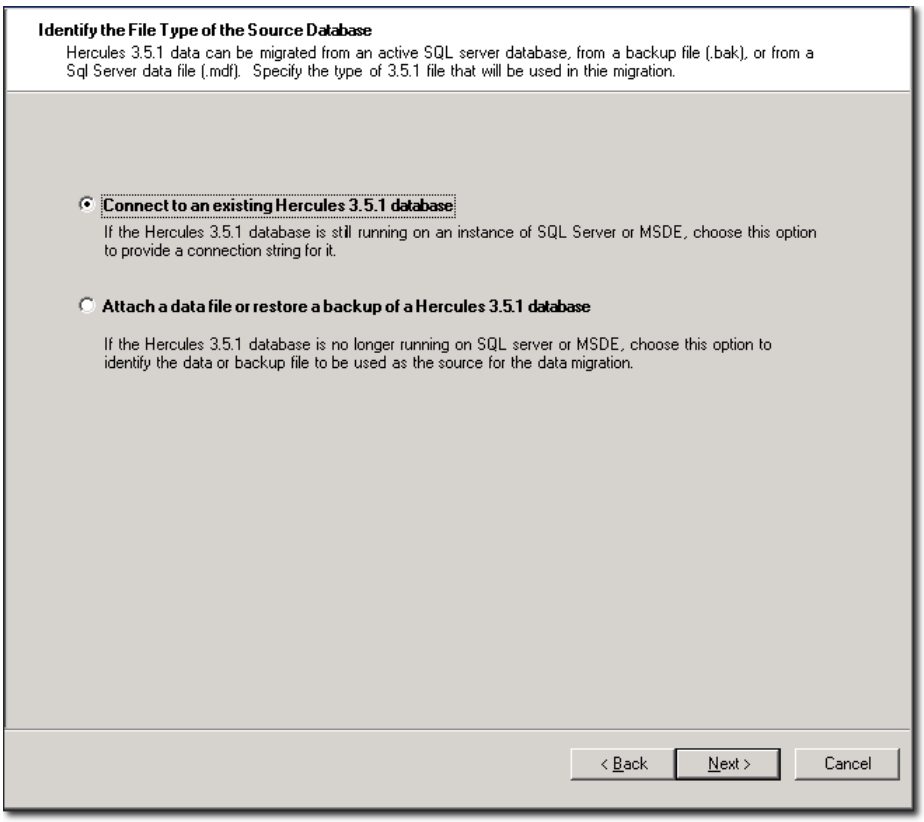


5. Click **Next**. Select **Migrate the Hercules database** to migrate all of the objects used in the Hercules Server, including all custom vulnerabilities, custom remedies, custom ActionPacks, policy enforcements, schedules, devices, custom device queries, device query collections, and more.



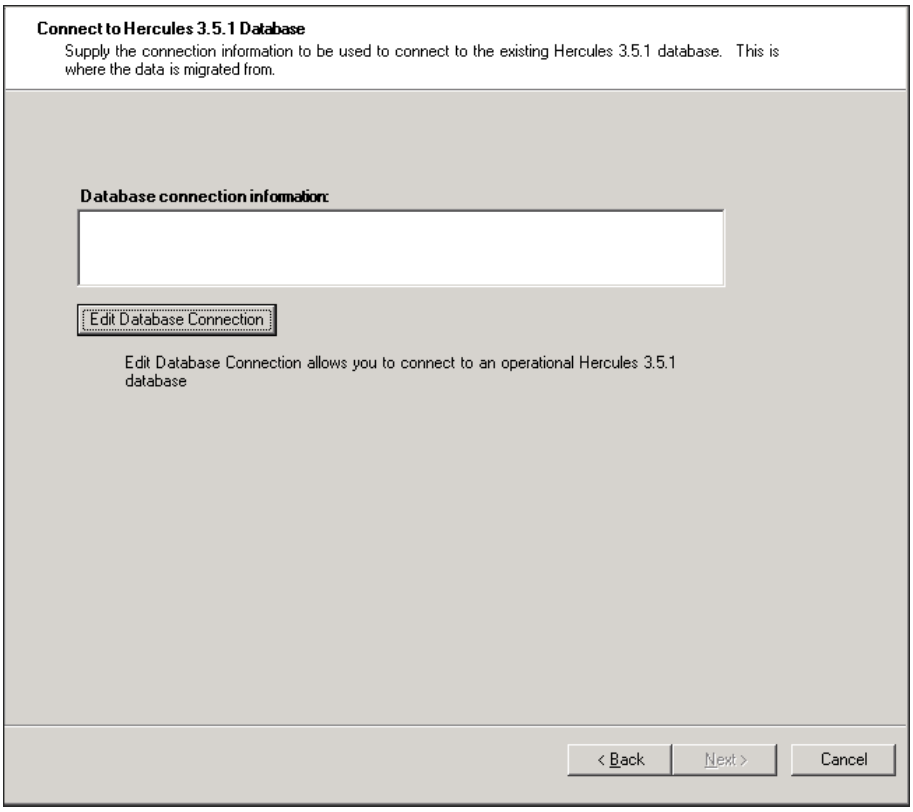
6. Click **Next** to display the page on which you identify the source from which to migrate the v3.5.1 Hercules database, where the source may be the active SQL database itself or a file (.mdf or .bak).
   - Select **Connect to an existing Hercules 3.5.1 database** if the Hercules v3.5.1 database is currently active and you are running a Hercules 4.0 server in parallel.

- Select **Attach a data file or restore a backup of a Hercules 3.5.1 database** if the Hercules v3.5.1 database is no longer running and the file to be used for data migration is either a Microsoft SQL Server Master Database file (.mdf) or a backup file (.bak).

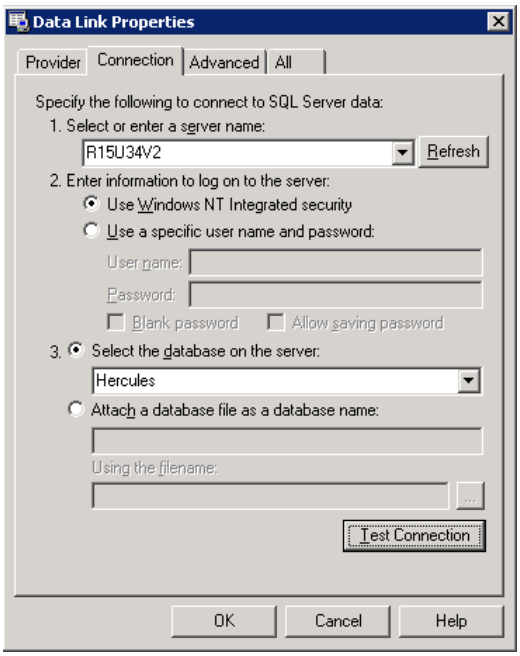


7. Click **Next.** Proceed as follows based on your last selection.
   - If you selected **Connect to an existing Hercules 3.5.1 database,** continue with Step 8.
   - If you selected **Attach a data file or restore a backup of a Hercules 3.5.1 database**, continue with Step 11.

8. If you selected Connect to an existing Hercules 3.5.1 database, a page displays where you supply connection information that enables connecting to the Hercules v3.5.1 database from which the data is migrated.

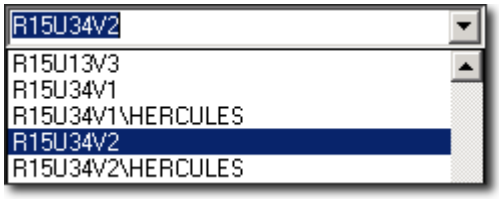


9. Click **Edit Database Connection** to open Data Link Properties - Connection tab.

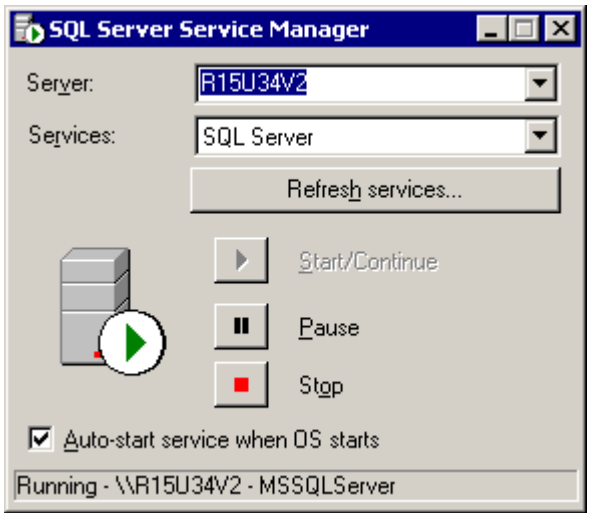


10. Complete the Data Link Properties for the source database as follows:

    a. For **1. Select or enter a server name**, enter or select the server name of the server where v3.5.1 is installed. Do *not* select the listed item with the server name followed by `\HERCULES`.



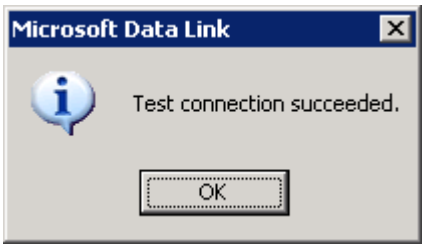
    If you don't remember, log on to this server and click the SQL Server icon in the system tray to display the SQL Server Service Manager and view the entry for Server.



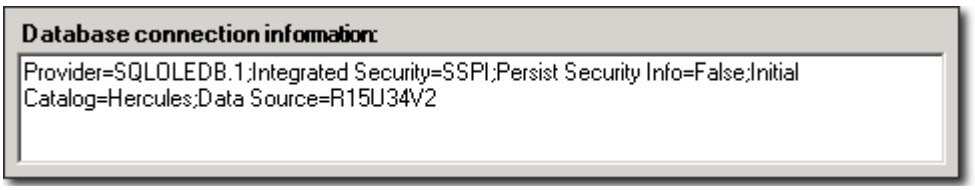
    b. For **2. Enter information to log on to the server**, select `Use Windows NT Integrated Security`, the default for Hercules authentication.

    c. For **3**, select **Select the Database on the Server**, and select **Hercules** from the pull-down list.

    d. Click **Test Connection**.

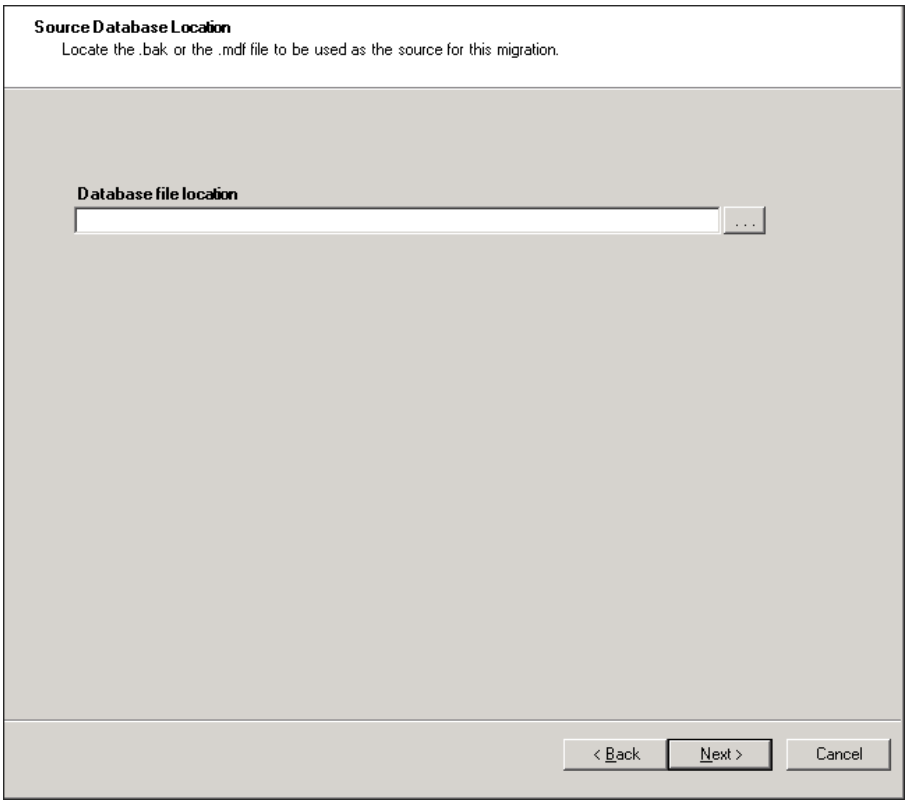


e. Click **OK**. Your entries on the Data Link Properties page are displayed in the Database connection information textbox. The following example is for selecting the database on the server.



f. Verify the entry then click **Next**. Continue with Step 14.

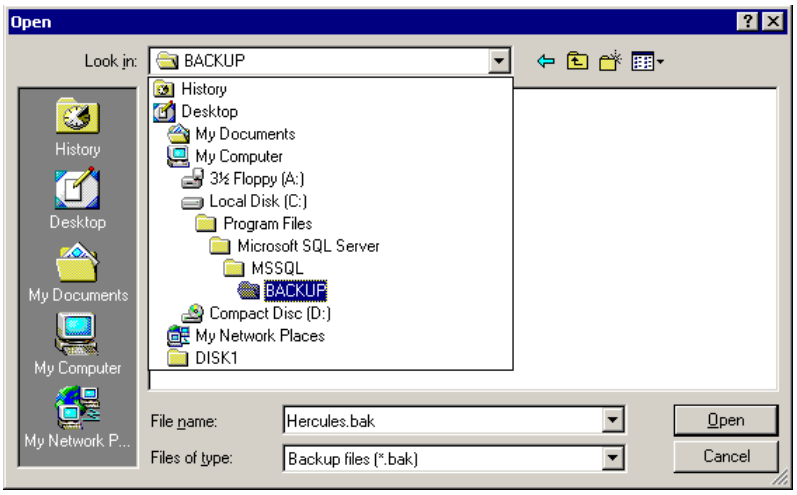
11. If you selected **Attach a data file or restore a backup of a Hercules 3.5.1 database**, the Source Database Location window appears.



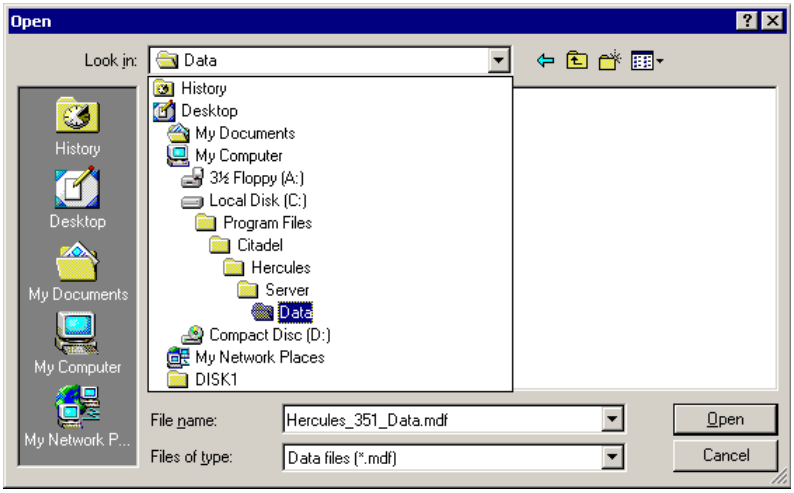
12. Click Browse and navigate to the .bak or .mdf file to be used as the source file for this migration and select it.

Tip - Using a database backup file is the better choice because backup files are much smaller than .mdf files. Also, the .mdf file may not be usable if the database was not properly detached.

- To migrate from a backup file, select Backup files (*.bak) for Files of Type, then navigate to the directory where the Hercules.bak file is stored. Highlight the filename and click **Open**.



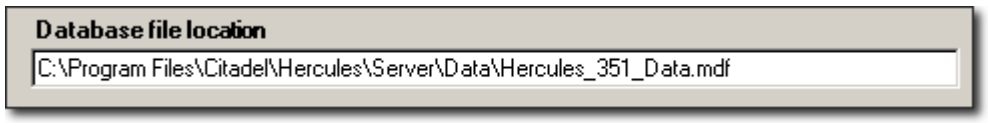
- To migrate from a data file, select Data Files (*mdf) for Files of Type, then navigate to the directory where the Hercules_351_Data.mdf file is stored. Highlight the filename and click **Open**.



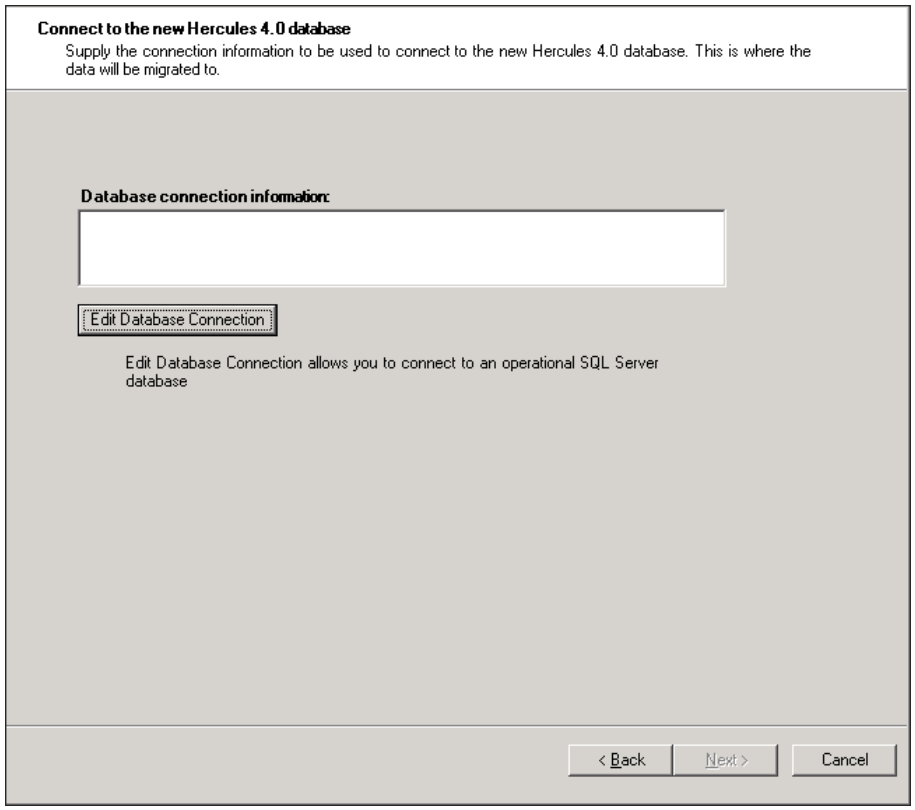
13. Verify database file location, then click **Next**.

- If migrating from a backup file, the path should resemble the following: `C:\Program Files\MicrosoftSQLServer\MSSQL\BACKUP\Hercules.bak`

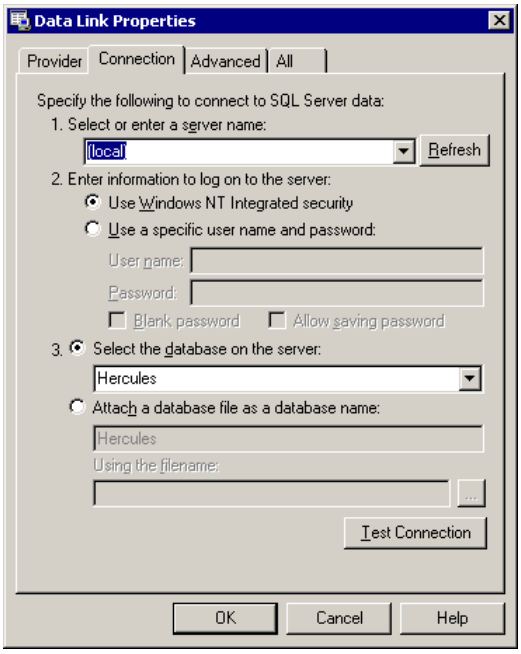
- If migrating from a data file, the path should resemble the following: `C:\Program Files\Citadel\Hercules\Server\Data\Hercules_351_Data.mdf`



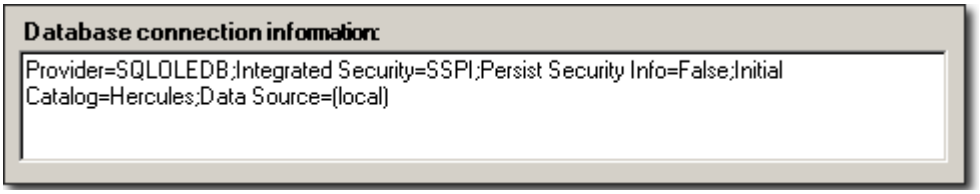
14. The Connect to the new Hercules 4.0 database page displays.



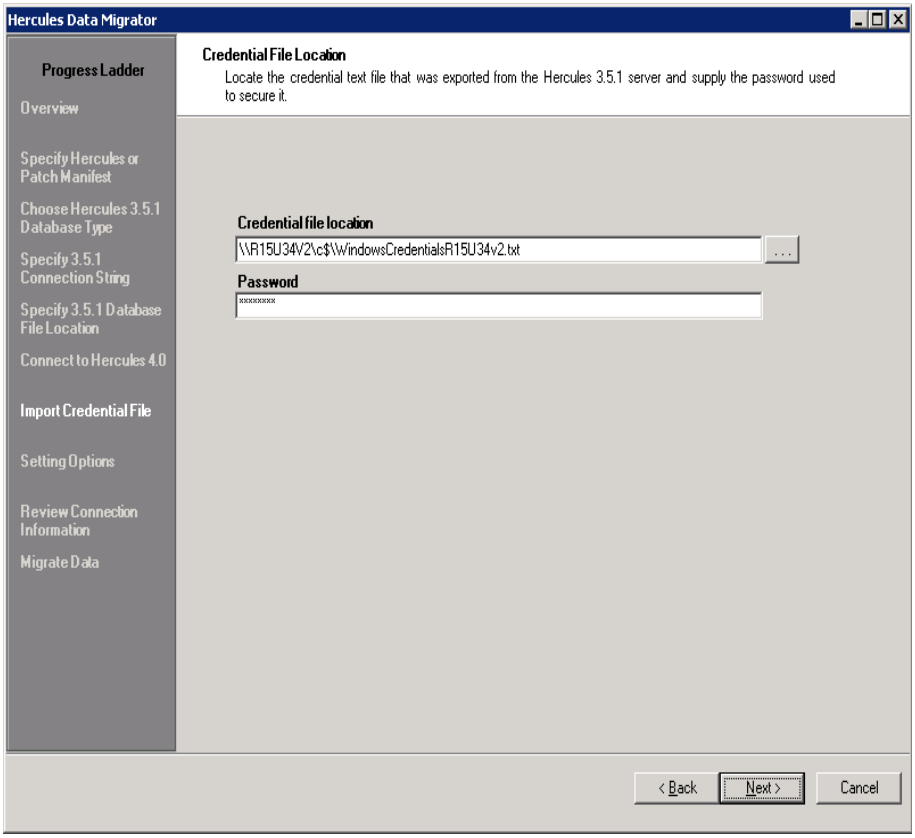
15. Click **Edit Database Connection** to open Data Link Properties for connecting to the Hercules v4.0 destination database.



16. Complete the Data Link Properties for the destination database as follows:
    a. Select **(local)** for the server name
    b. Select the security information used by the SQL server, normally **Use Windows NT Integrated security**.
    c. Select the database on the server. Typically, the name for the Hercules database is `Hercules`.
    d. Click **Test Connection**.
    e. Click **OK** to the confirmation message.
    f. Click **OK** to close the window and display the configured connection information in the Database connection information textbox.



17. Verify the entry, then click **Next**. The Credential File Location displays.



18. Complete the Credential File Location dialog as follows:
    a. For **Credential file location**, click **Browse** and navigate to the path where the Credential file resides, or, if you saved the file on the C:\ drive of the source machine, enter:

       `\\<servername>\c$\<credentialfile>.txt`

    b. For **Password**, enter the same password you entered for the Credential File Exporter. (See Step 2 in "Export Windows and Unix Credentials to a Local Text File" on page 5-13.)

    c. Click **Next**.

19. Consider whether the settings from the Hercules v3.5.1 server should be copied to the Hercules v 4.0 database based on the following.

    For the Hercules server, a copy overwrites the following:

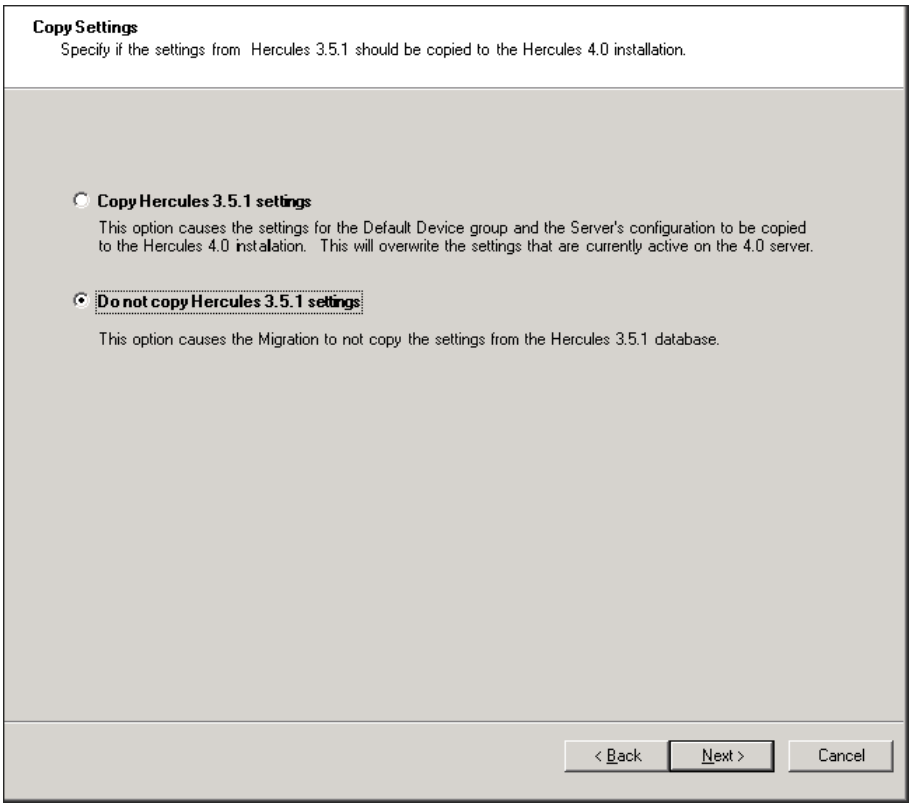
    - 'VFLASH.LastPollTime'
    - 'VFLASH.PollTimeOfDay'
    - 'VFLASH.MaxDatabaseBackups'
    - 'VFLASH.PollDays'

    For Hercules device groups, a copy overwrites the following:

    - PATCH_REPOSITORY
    - PROXY_ADDRESS
    - LOG_MAX_BYTES
    - POLICY_ID
    - ADMIN_REBOOT_MESSAGE
    - CLIENT_REBOOT_MESSAGE
    - _REBOOT_SECONDS
    - OPTIONS_CHECK_PERIOD
    - _CYCLE
    - CUSTOM_INSTALL_PATH
    - NOTE
    - REM_WARNING,
    - REM_DEFER
    - FIREWALL_LOCAL_NET
    - _LOCAL_NET_OVERRIDE
    - FIREWALL_HERCULES_NET
    - FIREWALL_HERCULES_NET_OVERRIDE
    - _UPDATE
    - ROLLBACK_TYPE_ID

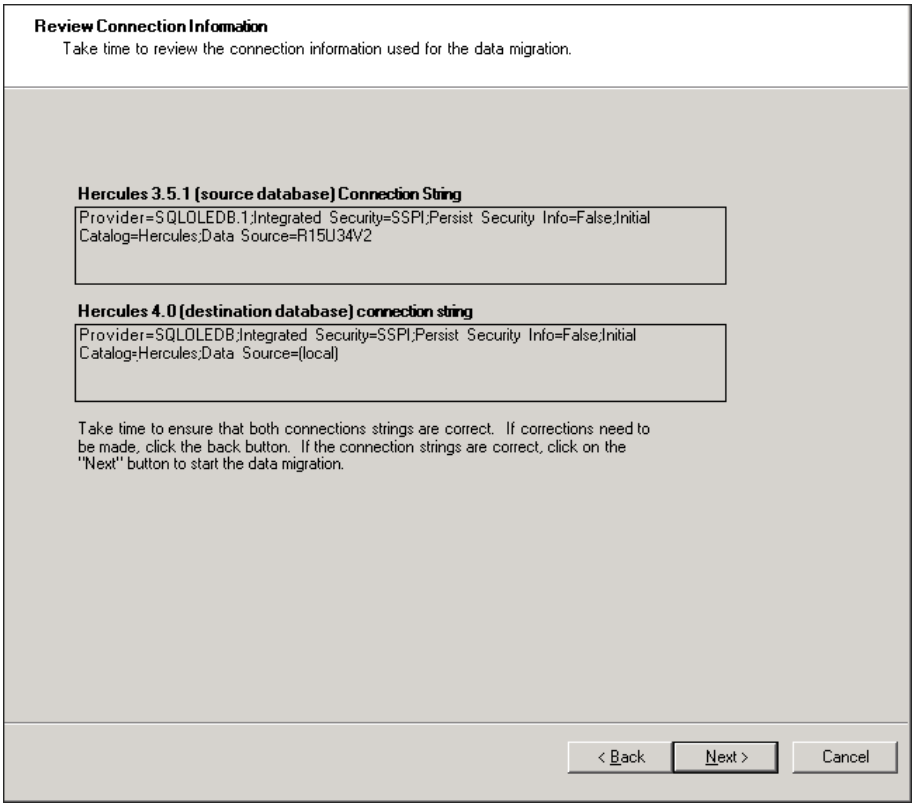
20. Specify if the settings from the Hercules v3.5.1 server should be copied to the Hercules v 4.0 database.
    - Select **Copy Hercules 3.5.1 settings** to copy the servers configuration.

- Select **Do not copy Hercules 3.5.1 settings** to continue the migration without copying the settings.

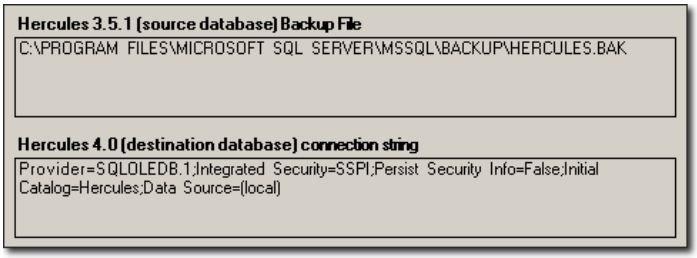


21. Click **Next**. Review connection information.

- If migrating from a source database, the information may resemble this:

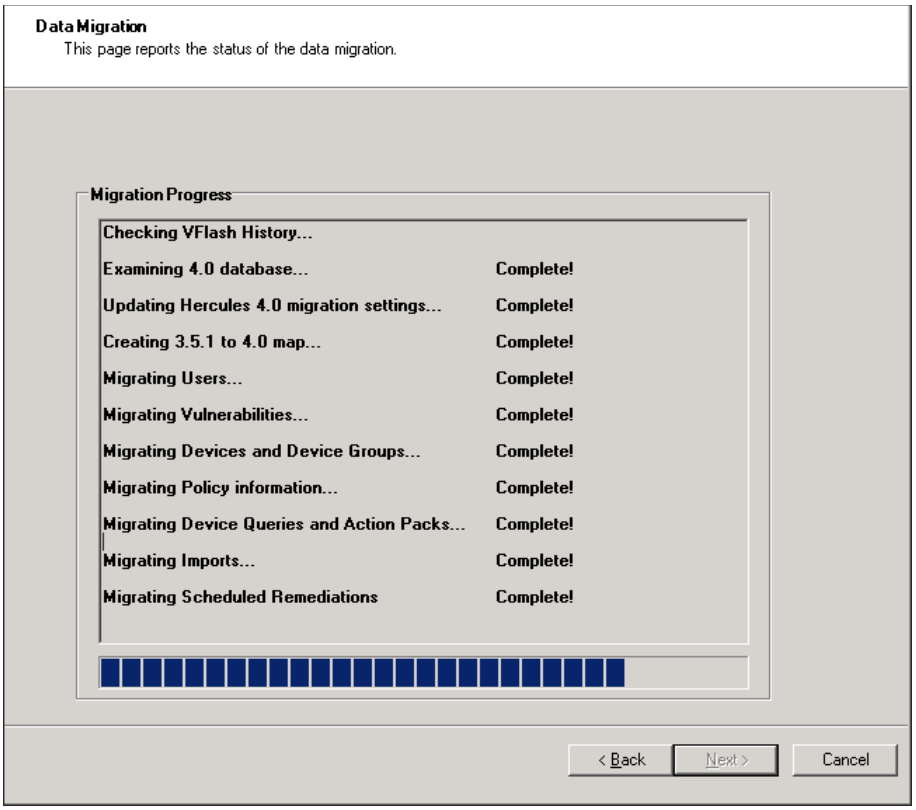


- If migrating from a backup file, the information may resemble this:

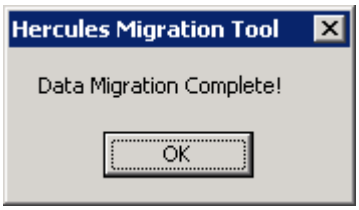


- If migrating from a data file, the information may resemble this:

22. Click **Next**.



23. Review data migration status.



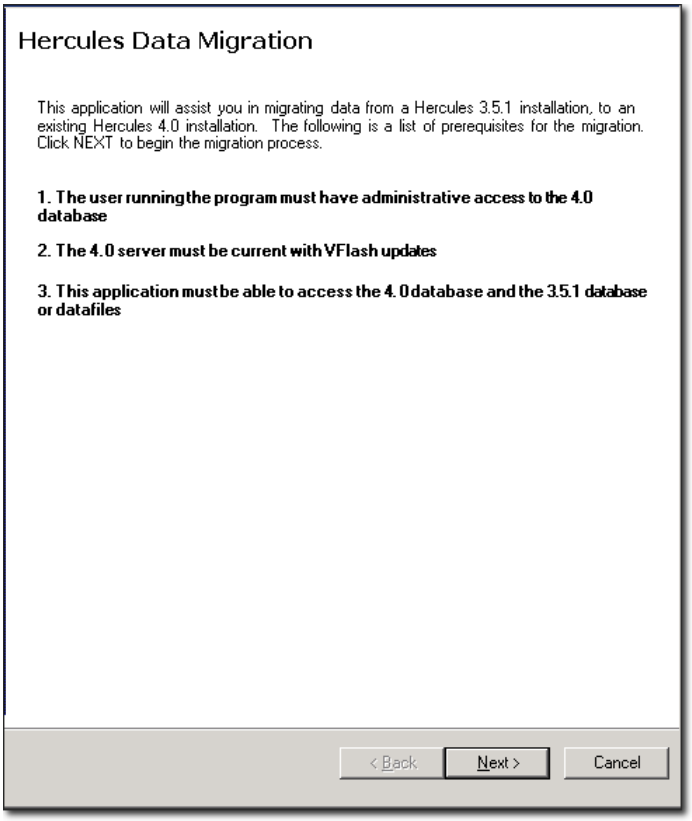
24. Click **OK** to the Data Migration Complete message. Then click **Finish**.

Migrate the Hercules Patch Manifest Database, Data File or Backup File

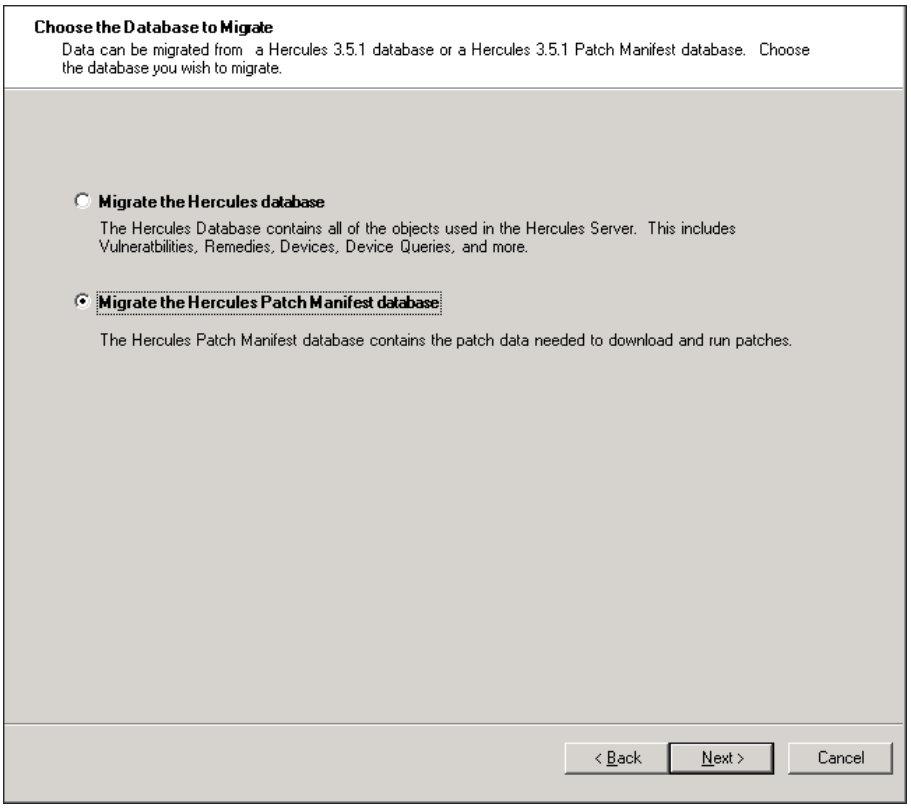
Patch Manifest migration includes records in the 3.5.1 Patch Manifest database that are not shipped with the destination Patch Manifest database, patch actions where the base URL is not equal to the custom URL, and user-defined scripts.

To use the Hercules Data Migration Tool to migrate the Patch database or file

1. Complete the preceding steps in the workflow for your migration strategy.
   - If migrating the Patch Manifest database, first complete Step 1 through Step 8 in "Migrating a v3.5.1 Source Database to a v4.0 Destination System" on page 5-3.
   - If migrating from a Patch Manifest backup file, complete Step 1 through Step 14 in "Migrating a v3.5.1 Source Backup File (.bak) to a v4.0 Destination System" on page 5-5.
   - If migrating from a Patch Manifest data file, complete Step 1 through Step 11 in "Migrating a v3.5.1 Source Database File (.mdf) to a v4.0 Destination System" on page 5-7.
2. Log on to the server where Hercules v4.0 Channel Server is installed.
3. From the **Start** menu, select **All Programs > Hercules > Data Migration Tool**.

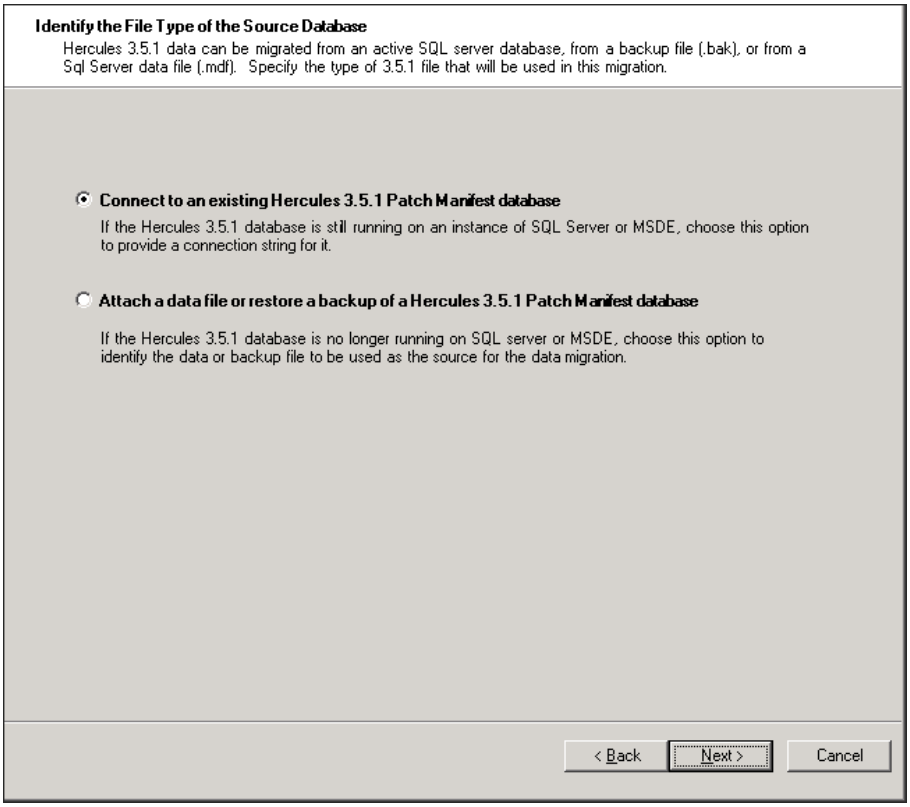


4. Click **Next**. Select **Migrate the Hercules Patch Manifest database** to migrate the patch data needed to download and run patches.



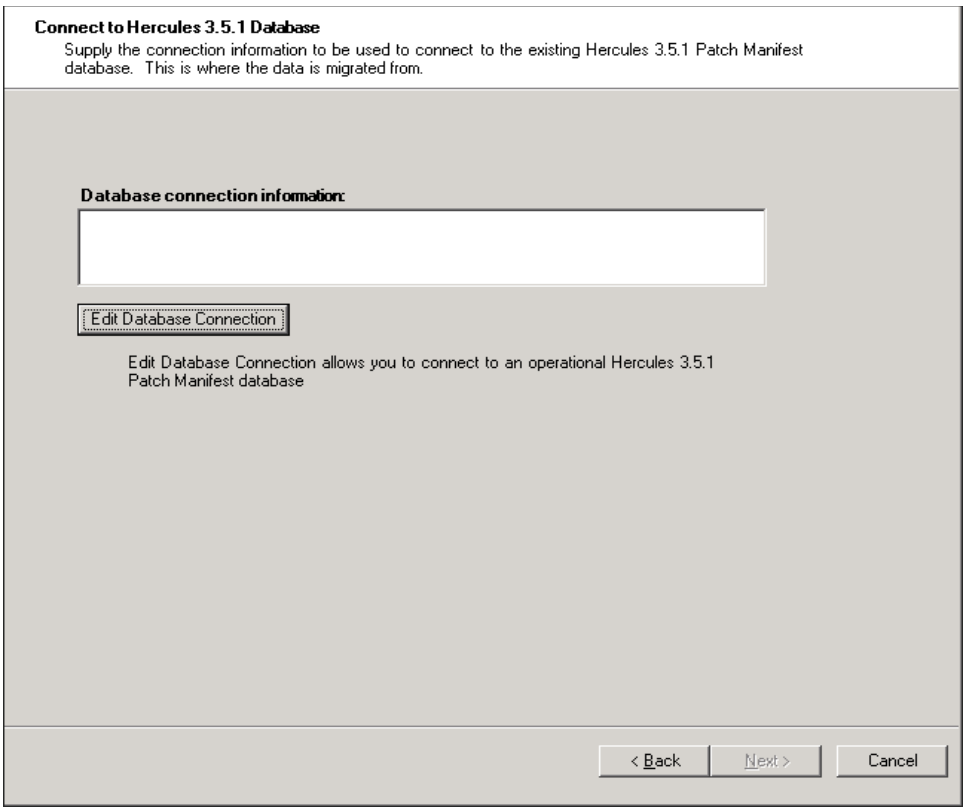
5. Click **Next** to display the page on which you identify the source from which to migrate the v3.5.1 Patch Manifest database, where the source may be the active SQL database itself or a file (.mdf or .bak).
   - Select **Connect to an existing Hercules 3.5.1 Patch Manifest database** if the Hercules v3.5.1 Patch Manifest database is running on an active SQL server or MDSE. This is the right choice if you are running the old and new release in parallel.

- Select **Attach a data file or restore a backup of a Hercules 3.5.1 Patch Manifest database** if the Hercules v3.5.1 database is no longer running and the file to be used for data migration is either a Microsoft SQL Server Master Database file (.mdf) or a backup file (.bak). This is the right choice if you are upgrading in place on the same server.

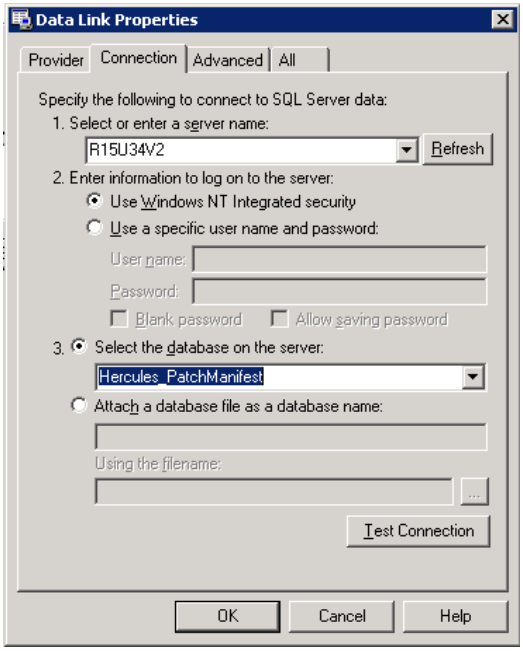


6. Click **Next.** Proceed as follows based on your last selection.
   - If you selected **Connect to an existing Hercules 3.5.1 Patch Manifest database,** continue with Step 7.
   - If you selected **Attach a data file or restore a backup of a Hercules 3.5.1 Patch Manifest database**, continue with Step 10.

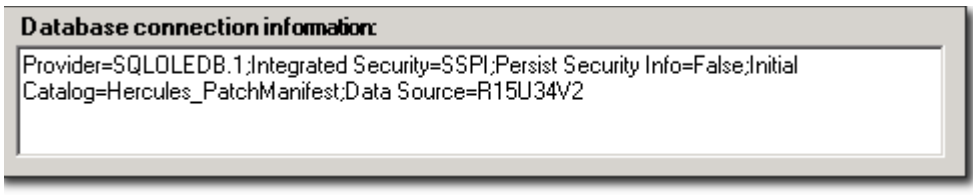
7. If you selected Connect to an existing Hercules 3.5.1 Patch Manifest database, a page displays where you supply connection information that enables connecting to the Hercules v3.5.1 Patch Manifest database from which the data is migrated.



8. Click **Edit Database Connection** to open Data Link Properties - Connection tab for the source data.

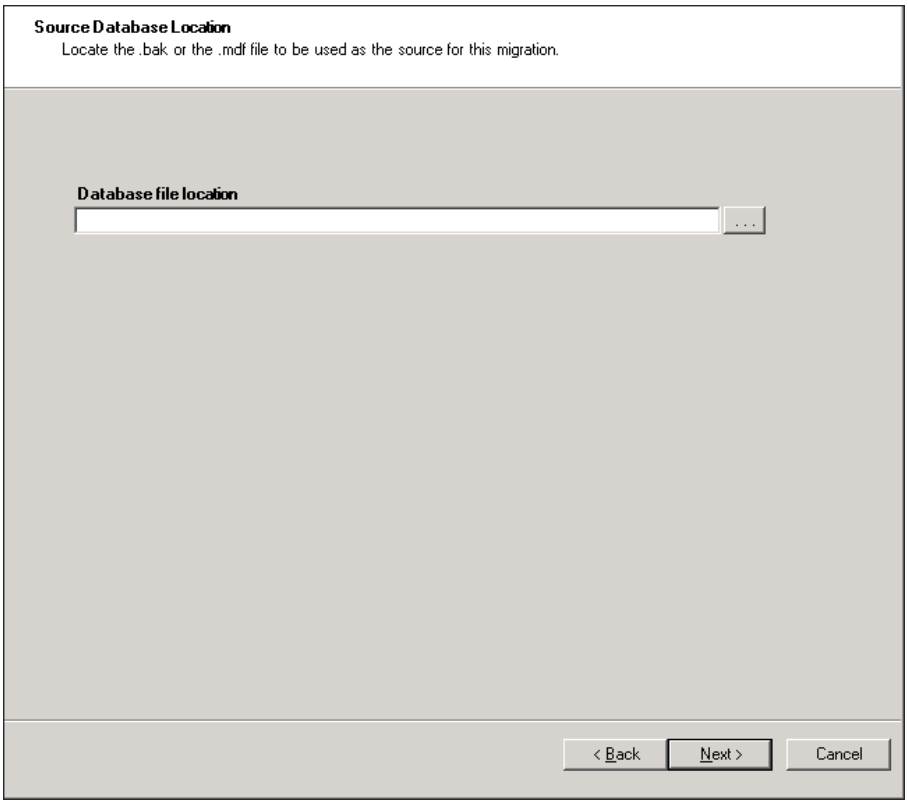


9. Complete the Data Link Properties for the source database as follows:
   a. For **Select or enter a server name**, enter or select the server name of the server where v3.5.1 is installed.
   b. For **Enter information to log on to the server**, select `Use Windows NT Integrated Security`, the default for Hercules authentication.
   c. For **Select the Database on the Server**, select the **`Hercules_PatchManifest`** database from the dropdown list.
   d. Click **Test Connection**. Click **OK** to the confirmation message.
   e. Click **OK**. Your entries on the Data Link Properties page are displayed in the Database connection information textbox.



   f. Verify the entry, the click **Next**. Continue with Step 13 on page 5-41.

10. If you selected **Attach a data file or restore a backup of a Hercules 3.5.1 database**, the Source Database Location window appears.



11. Click **Browse,** and navigate to the location of the desired file, and select it.
    - To migrate from a backup file, select Backup files (*.bak) for Files of Type, navigate to the source directory, highlight the filename, `PatchManifest.bak`, and click **Open**. The default path for backups created with the SQL Enterprise Manager is:

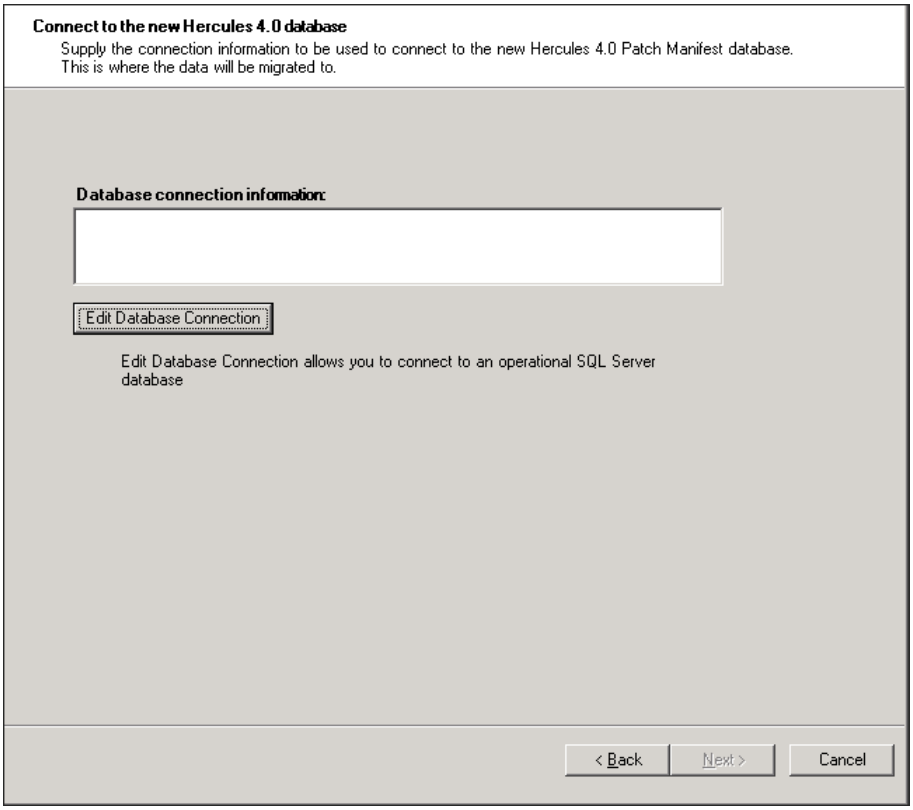
      `C:\Program Files\Microsoft SQL Server\MSSQL\BACKUP`
    - To migrate from a data file, select Data Files (*mdf) for Files of Type, then navigate to the source directory, highlight the filename, `Hercules_PatchManifest_351.mdf`, and click **Open**. The default path is:

      `C:\Program Files\Citadel\Hercules\Server\Channel Server\Data`

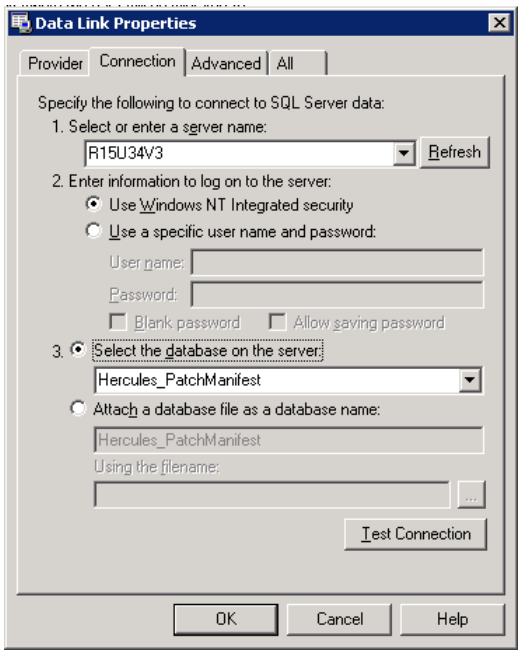
Tip - Selecting PatchManifest.bak is the better choice because this backup file is much smaller than the Hercules_PatchManifest_315.mdf file. Also, the .mdf file may not be usable if the database was not properly detached.

12. Verify the database file location and click **Next.**

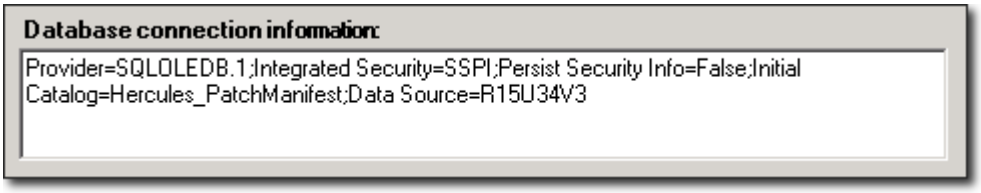
13. The Connect to the new Hercules 4.0 database page displays.



14. Click **Edit Database Connection** to open Data Link Properties for connecting to the Hercules v4.0 destination database.

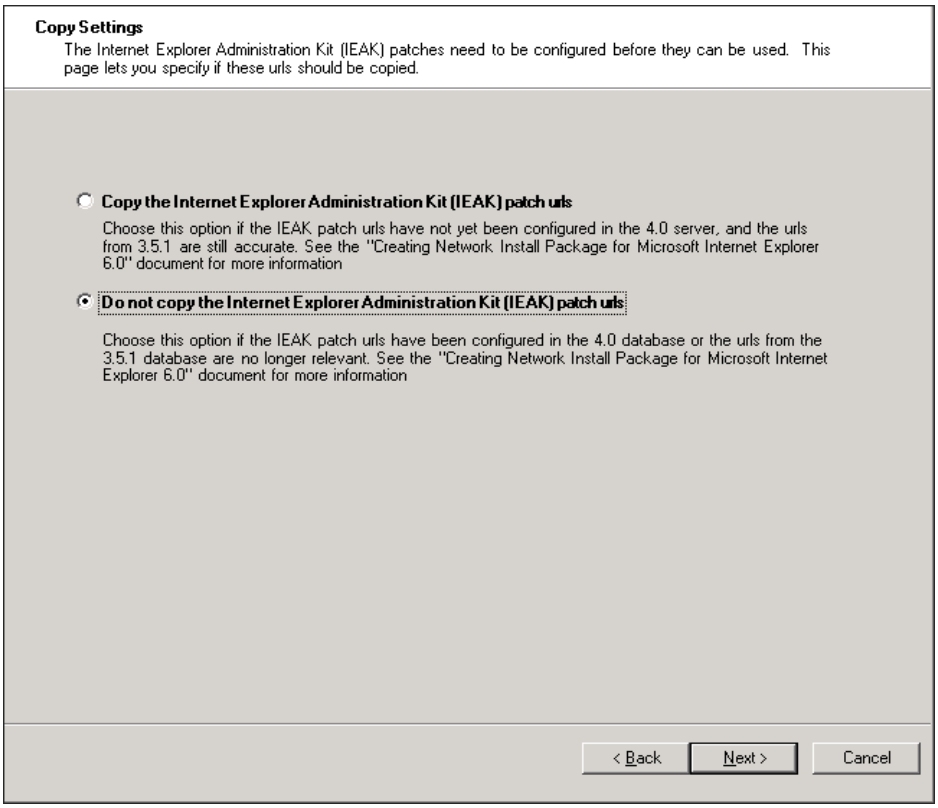


15. Complete the Data Link Properties for the 4.0 database as follows:
    a. Select the name of the destination server for the server name.
    b. Select the security information used by the SQL server, normally **Use Windows NT Integrated security**.
    c. For **3**, select **Select the database on the server**. Typically, the name for the destination Hercules database is `Hercules_PatchManifest`.
    d. Click **Test Connection**.
    e. Click **OK** to the confirmation message.
    f. Click **OK** to close the window and display the configured connection information in the Database connection information textbox.

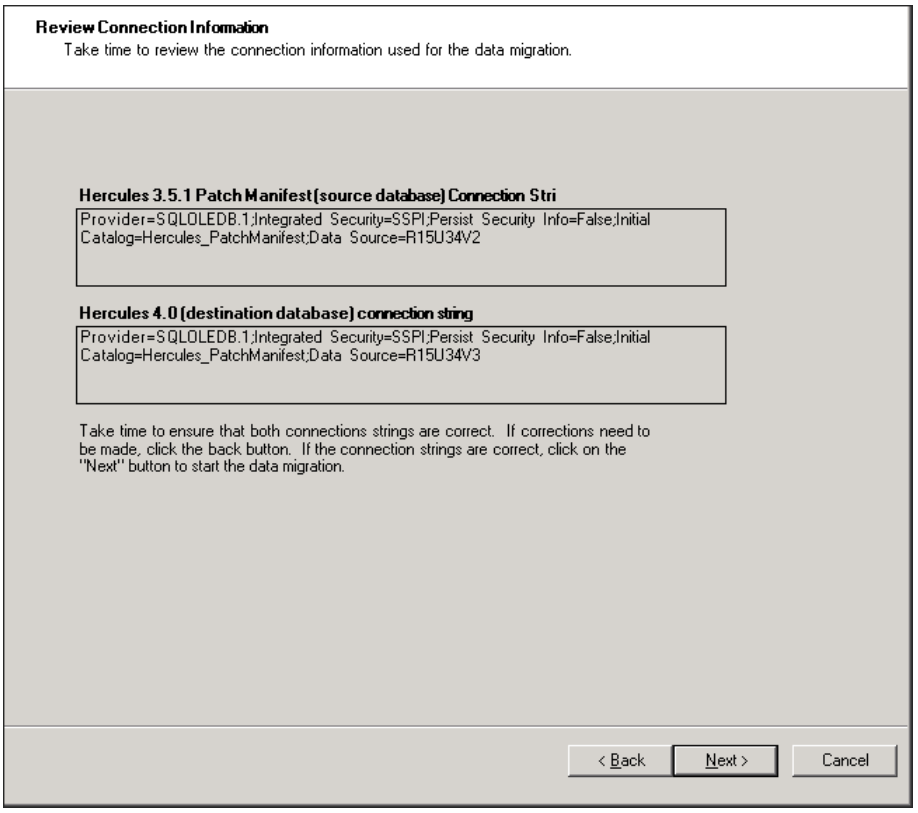


16. The Copy Settings page displays. Consider whether to copy the Internet Explorer Administration Kit (IEAK) patch URLs based on whether they have already been configured in v4.0. If not, select the option to copy these URLs.
17. Specify whether the IEAK patch URLs are to be copied.
    - Select **Copy the Internet Explorer Administration Kit (IEAK) patch urls** if you have not yet created the installation package for IE SP 1 as described in "Create the Network Install Package for Microsoft IE 6.0" on page 3-1.

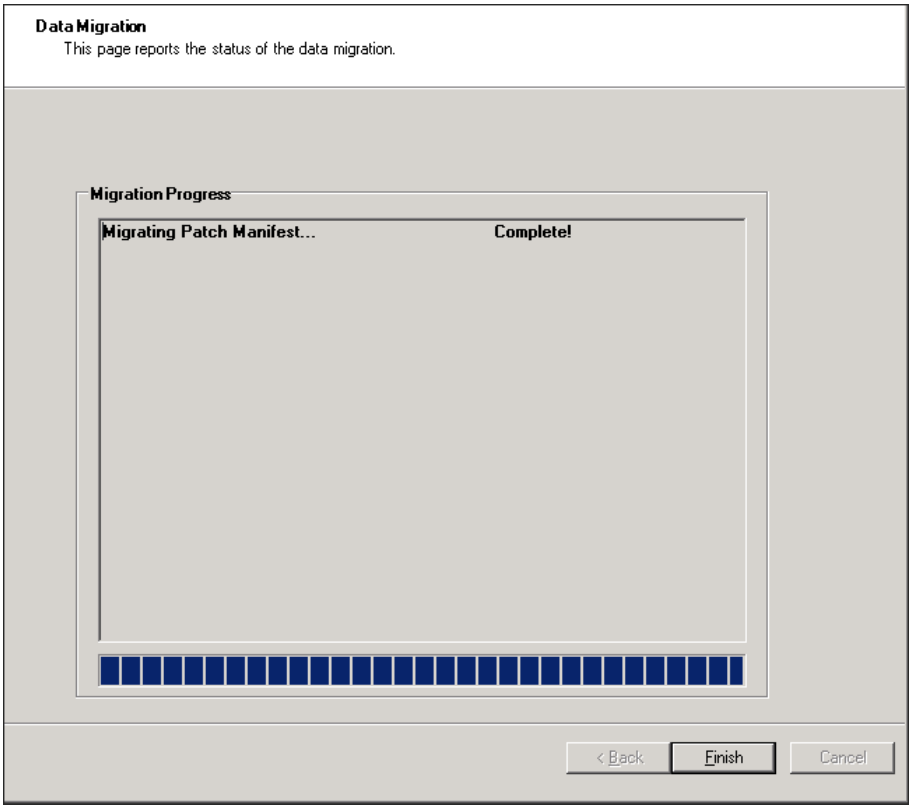
- Select **Do not copy the Internet Explorer Administration Kit (IEAK) patch urls** if the patch URLs have been configured in the 4.0 database or the URLs from the 3.5.1 database are no longer relevant.



18. Click **Next**. Review connection information. An example for migrating across servers follows:



19. Click **Next**. Review data migration status.



20. Click **Finish**.

Perform Post-Migration Setup

This section addresses the following topics:

- "Ensure v3.5.1 Clients Update to v4.0 and Check in with v4.0 Servers"
- "Consider User Passwords"

Ensure v3.5.1 Clients Update to v4.0 and Check in with v4.0 Servers

Use the following procedure only if your migration was performed from one server to another. If you migrated in place, this procedure is not necessary.

The migration process replaces migrated Device Groups' Download Serer URL with the Download Server URL of the Default Device Group. If you have multiple Hercules Download Servers and want to distribute device groups among them, you must manually change the Download server URL setting in Device Group Properties for each Device Group.

To upgrade v3.5.1 Hercules Clients

1. Open a v.3.5.1 Hercules Administrator and connect to a v3.5.1 Hercules server to which clients are currently checking in.
2. From the Navigation pane under Device, select **Device Group**s to open Manage Device Groups.
3. For each device group listed, click **Properties**, click the Device Preferences tab, and do the following:
   a. Change the **Hercules server URL** from the URL of the v3.5.1 Hercules server to the URL of the v4.0 Hercules server.
   b. Verify that the checkbox is checked for **Automatically update client when a newer one becomes available**.
   c. Record the entry for **Client installation location** if changed from the default. You will need to enter this path in the corresponding field of the Device Group Properties in the v4.0 Hercules Administrator.
4. Close the v3.5.1 Hercules Administrator.
5. Open the v4.0 Hercules Administrator.
6. If you recorded 3.5.1 entries for Client installation location, for each Device Group, enter the corresponding path for Client installation location.
7. If your v4.0 system has multiple Hercules Download Servers, modify the Download server URL for each Device Group that uses a different download server than the default group as follows:
   a. From the Navigation pane under Device, select **Device Group**s to open Manage Device Groups.
   b. For each Device Group, click **Properties**, click the Device Preferences tab, edit the Download server URL as needed, click **Test** to verify the connection. Click **OK**.

Consider User Passwords

Hercules User IDs, configured under Users and Security for the Hercules server, are migrated. The default authentication for Hercules 4.0 Users is Hercules Integrated Authentication, which requires configuration of a password, whereas Hercules 3.5.1 used Windows Integrated Authentication, where configuration was just the Windows domain\username and the password configured for Windows was used.

If you plan to adopt the default Hercules Integrated authentication for your v4.0 system, the Hercules User IDs that are migrated have blanks for passwords. Hercules users can log on with the blank password and change their password or a Hercules Administrator can reset the Hercules password for any Hercules user.

To override the default and continue using Windows Authentication with Hercules v4.0, navigate to `C:\Program Files\Citadel\Hercules\Server\Configuration` and run `SetAuthentication.exe`

A. Removing Software Permanently

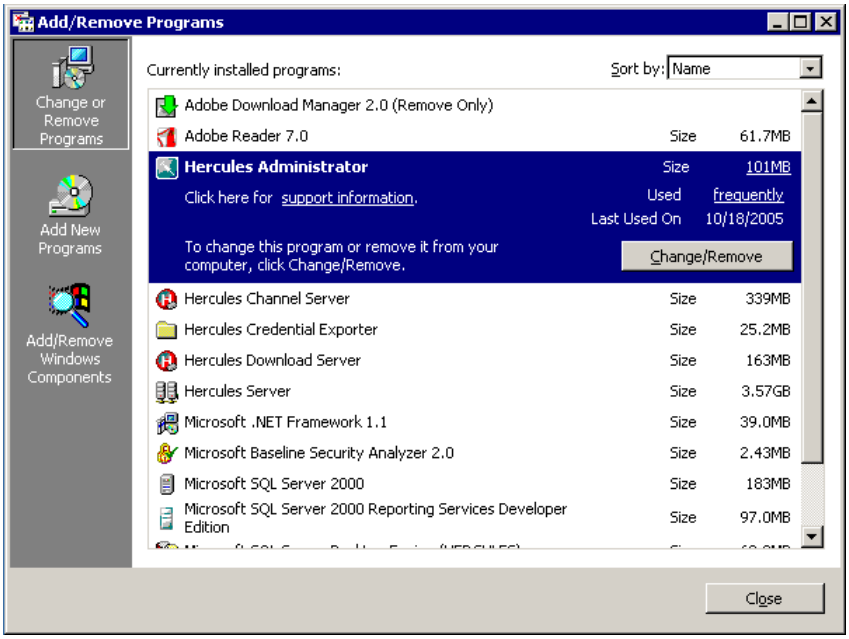
Remove Hercules software from a server based on your migration strategy. Examples of when to remove software follow:

- After making a backup of your 3.5.1 Hercules databases and before installing the Hercules 4.0 system on the same server and using the Migration Tool to restore your backup files.
- Before installing the Hercules 4.0 system on the same server and using the Migration Tool to reattach your *.mdf files.
- After you have successfully migrated your Hercules 3.5.1 data to the server on which the Hercules 4.0 system is running.

To manually uninstall the Hercules Server, the Hercules Download Server, or the Hercules Channel Server, use the **Add/Remove** program in the Control Panel.

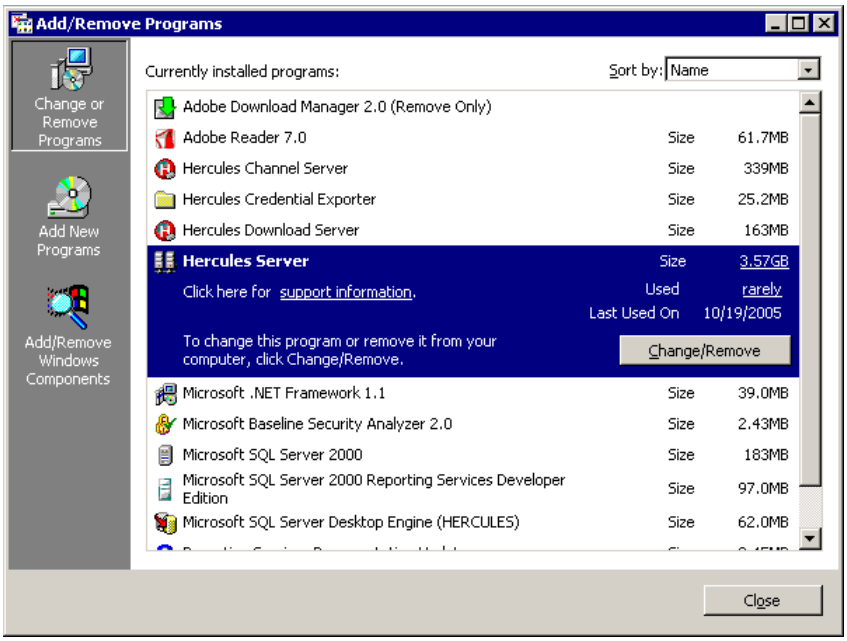
To completely remove the Hercules software from your system

1. Click the Windows **Start** button, **Settings** (if on Windows 2000), and select **Control Panel**.
2. Double-click the **Add/Remove Programs** icon.
3. If the Hercules Administrator is installed, highlight it.

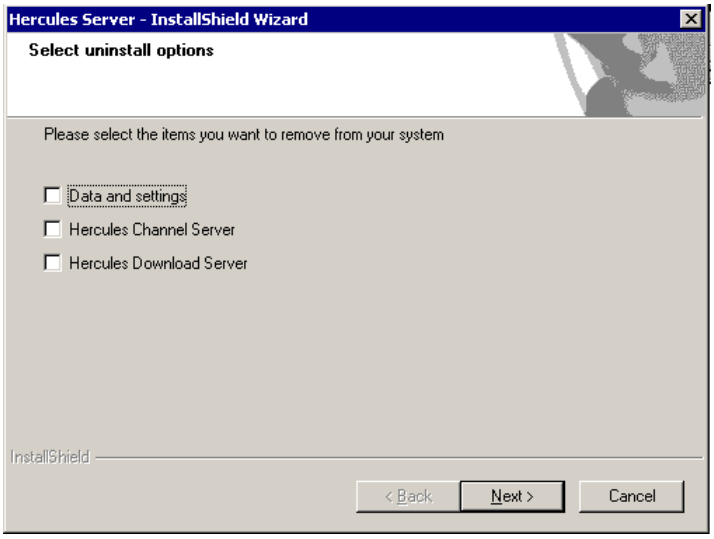


4. Click **Change/Remove** to start the InstallShield Wizard.
5. Click **OK** to confirm the uninstall and display the uninstall progress on the Wizard Setup Status page.

6. When processing completes, click Finish. The server reboots.
7. Log back on and redisplay Add/Remove Programs.

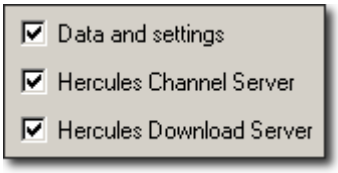


8. From the list, select **Hercules Server**. (This option uninstalls the Hercules Channel Server and Hercules Download server as well if you installed in a standalone environment.)
9. Click **Change/Remove**.
10. When the Confirm Uninstall message displays, click **OK**. The Select uninstall options page displays.

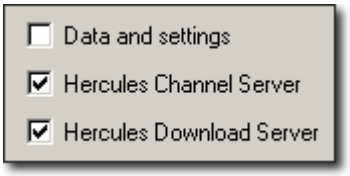


11. Select the items to remove from your system as follows based on the type of migration you are performing.

- If planning to migrate from a backup file, check all three options.



- If planning to migrate from an *.mdf file, leave Data and settings unchecked.



- If you have already migrated data and settings to a new server and you no longer need this previous installation, check all three options.

12. Click **Next.** View the progress shown on the Setup Status displays.
13. In the InstallShield Wizard Maintenance Complete page, click **Finish**.

References

References to third-party vendor documentation and Internet sites are subject to change without notice. Alternate paths are provided to help you find the sources in the event the links become disabled.

Adobe Systems Incorporated

Download Adobe Reader

http://www.adobe.com/products/acrobat/readstep2.html

Hewlett-Packard

Download latest patches for HP-UX 11.0 and 11i v1

Download required patches from http://www.itrc.hp.com

Microsoft Corporation

Services required to run security-enhanced IIS server on Windows 2000

http://support.microsoft.com/default.aspx?scid=kb;en-us;810866

Or, navigate in your Internet browser to http://www.support.microsoft.com and search the Knowledge Base for article 810866.

Download Microsoft NET v1.1 Framework

http://www.microsoft.com/downloads/details.aspx?FamilyID=262d25e3-f589-4842-8157-034d1e7cf3a3&displaylang=en

Download Windows 2000 High Encryption Pack

http://www.microsoft.com/windows2000/downloads/recommended/encryption/download.asp

Glossary

Access Control List (ACL)

In a Cisco Network Admission Control (NAC) environment, one or more lists used by a Network Access Device (NAD) to permit or deny access to the network device objects. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges or roles. Typically, the NAD is a Cisco Internet Operating System (IOS) router.

Access Control Server (ACS)

The Cisco Secure policy server in a Cisco Network Admission Control (NAC) framework. The ACS evaluates the posture credentials it receives from the Network Access Device (NAD) and forwards the credentials to the Hercules Posture Validation Server (PVS) on the Hercules Server for validation.

ActionPack

A group of vulnerabilities associated with a device query that is provided by Citadel or is user-defined. During policy enforcement, the ActionPack lets you apply remedies to devices that match a specific device query criteria, thus allowing for accurate application of corporate security configuration and/or profiles.

ActionPack catalog

A list of Citadel-provided ActionPacks available to use as a basis for remediation or policy enforcement.

AssetGuard

A licensed Hercules® capability that uses device inventory, device query, ActionPacks, and policies to enable you to quickly identify and remediate new vulnerabilities. The inventory data allows you to perform detailed queries to rapidly identify devices to include in an ActionPack for future policy enforcement.

Cisco Trust Agent (CTA)

A software tool in the Network Admission Control (NAC) environment located on the Hercules Client device that collects posture credentials (state information) from the client device and forwards the information to the Network Access Device (NAD), typically a Cisco router.

Client Management Service (CMS)

A Hercules service that enables you to control Hercules Clients that are installed on devices in your network. The CMS supports Hercules Clients for devices using Microsoft Windows, UNIX, and Linux operating systems.

Common Vulnerabilities and Exposures (CVE)

A community project that provides a dictionary of standardized names for vulnerabilities and other identified security exposures, making it easier for commercial products and research projects to share data and identify vulnerabilities consistently. A community-wide effort with representatives from security organizations such as security tool vendors, government agencies, academic institutions, and individual security experts makes this dictionary possible.

compliance checking

Evaluates the status of devices and determines whether they are compliant or noncompliant.

compliance only mode

Operation of the base Hercules product without licensing the Remediation feature. Compliance checking can be performed, but detected vulnerabilities cannot be automatically remediated.

Connect Guard

A host-based quarantine and remediation feature of the Hercules system that blocks network traffic from remote and local client devices reconnecting to the network, checks for security policy compliance, and applies the appropriate Network Access Policy (NAP) along with its remedy actions to noncompliant machines.

core features

Base Hercules features that are not specifically licensed. Core features include device discovery, device groups, device query, device logging, ActionPack catalog, policy catalog, vulnerability catalog, remedy catalog, compliance checking, and importing scan output files containing devices and detected vulnerabilities.

dashboard

The default display of the Hercules Operations Center that can include up to three user-selected instrument clusters, most of which are graphical representations of device security metrics. Selectable options include Message Center, Device Status, Device Vulnerability, Policy Compliance, Risk Assessment, ActionPack Hits, and Return On Investment Calculator.

detected vulnerabilities

Vulnerabilities detected on a device based on an import session or a compliance check. Vulnerabilities are grouped by High, Medium, and Low severity.

device

A computer in your enterprise that requires compliance monitoring, policy enforcement, or remediation of detected vulnerabilities.

device action

An action on a single device or on all devices within a device group, including installing or uninstalling Hercules Clients on devices, starting or stopping Hercules Clients, rebooting and remediating devices, collecting device inventory data, plus rolling back remediations and policy enforcements on devices.

device discovery

A Hercules function that discovers devices on your network that are in Windows Active Directory® domains, Windows NT® domains, or within a specified IP address range. You can also import device data directly from flat files.

device group

A grouping of devices based on a common criteria, such as departments, geographical locations, and enterprise architecture. Device groups help you organize and manage devices by allowing you to configure device properties at a group level or use them in device queries.

device inventory

A Hercules function that collects inventory information on the hardware and software installed on devices or the services (processes) running on devices. You can use inventory data in device queries to create more powerful ActionPacks. You must have an AssetGuard license to use device inventory.

device query

A Hercules function that searches the Hercules database for devices that match a specific set of criteria based on device properties and inventory data. You can manage individual device queries within a device query collection.

digital signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped.

Digital Signature Standard (DSS)

The digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents. DSS has become the United States government standard for authentication of electronic documents.

endpoint security

A method of protecting your network from potential security risks carried by devices attempting to join your network. A Network Access Policy (NAP) can be applied to devices secured by either the Hercules ConnectGuard feature or the Cisco Network Admission Control (NAC) solution.

enterprise reports

A license-based feature of the Hercules system that provides aggregate or roll-up data from different SQL report servers across multiple Hercules Servers. An Enterprise Reporting license is required for each Hercules Server that is configured for Enterprise Reporting.

Hercules Administrator

An administrative console from which you can manage one or more Hercules Servers, the Hercules Channel Server, one or more Hercules Download Servers, and other Hercules security components. You can also control and monitor Hercules operations from this console.

Hercules appliance

A single-blade server device that can be mounted in a Telco™ Style or 19-inch width rack. The appliance is preconfigured with Hercules software that enables Hercules users to perform server setup, device discovery, device configuration, inventory, ActionPack, policy and remedy management, policy and ActionPack enforcement, vulnerability assessment and remediation, compliance checking, and network monitoring and reporting.

Hercules Channel Server

The Hercules component that maintains the File Download Catalog, a list of URLs that Hercules remedies use to install patches, applications, scripts, and other files. The Hercules Channel Servers also coordinate activities on Hercules Download Servers.

Hercules Client

The Hercules software installed on a device that is running on a Microsoft Windows, UNIX, and Linux operating systems. The Hercules Client permits the Hercules Server to manage the device and perform device actions.

Hercules Download Server

A Hercules component that downloads and stores files such as patches, applications, or documents on behalf of Hercules Channel Servers.

Hercules Posture Plug-in (HPP)

In a Cisco NAC environment, a plug-in installed on the Hercules Client device that provides a bridge between the Hercules Client and the Cisco Trust Agent (CTA) residing on the client device. The HPP sends the client device's posture credentials (state information) including the client's installed version number and Global Unique Identification (GUID) number to the Cisco Trust Agent on the CTA.

Hercules Posture Validation Server (PVS)

In a Cisco Network Admission Control (NAC) environment, a Hercules Server component that validates the posture credentials of the Hercules client device it receives from the Cisco Access Control Server (ACS).

Hercules Role

A class of Hercules user that is allowed to perform certain tasks on a Hercules Server. The Hercules system provides several pre-defined roles and allows you to create custom roles using pre-defined Hercules tasks. The Hercules system administrator role can perform any task in the system. The Hercules Server administrator role can perform any task, except create, modify, and assign custom roles.

Hercules Security Asset

Any Hercules component or feature including servers (Hercules Server, Hercules Download Server, Hercules Channel Server), devices, device groups, remedies, policies, remediations, ActionPacks, and vulnerabilities defined in the Hercules system.

Hercules Security Portal

Citadel's information portal that contains the latest news of interest to security professionals, including virus information, security alerts, and a calendar of security-related events.

Hercules Server

The Hercules component that manages devices, vulnerabilities, and remedies, performs remediations and policy enforcements, and generates reports.

Import Session

A Hercules function that uses an import wizard to copy the results of a network device scan from a third-party scanner into the Hercules database. The results include detected vulnerabilities and data on the scanned devices. You can review the results of each import session.

licensed features

Hercules features that extend the functionality beyond the core features for an additional cost. Examples of licensed features are remediation, V-Flash, ConnectGuard, Cisco NAC, Asset Guard, and enterprise reporting.

logging

Hercules Clients collect and log device-specific information at the start of a remediation and when an error occurs. Before a remediation, the Hercules version number, operating system, host name, IP address, and MAC address of the device is captured on the device log. Device logs are transmitted to the Hercules Server when an error occurs or when the log file reaches the maximum size.

Network Access Device (NAD)

A device (typically a Cisco router) that receives forwarded information (client posture credentials or state information) from a Hercules client device about other client devices.

Network Access Policy (NAP)

A Citadel-provided or a user-defined policy that can be selected to be the NAP to apply on all devices managed by a Hercules Server, on all devices in a device group, or on a single device each time the device(s) attempt to access the network. A NAP can be configured for a device only if the Hercules ConnectGuard feature or the Cisco NAC feature is enabled on the device as the endpoint security method.

Network Admission Control (NAC)

An industry-wide effort led by Cisco Systems to help ensure that every endpoint device complies with network security policies before being granted access to the network. In a Hercules network containing Cisco components such as Cisco routers and Secure Access Control Servers, NAC can be configured as the endpoint security method to ensure that only client devices that fully comply with the appropriate Network Access Policy (NAP) are permitted to access the network.

OpenSSH

A free version of the SSH protocol suite of connectivity tools configured on Hercules Clients running on UNIX or Linux operating systems that are deployed via the Client Management Service (CMS). The Open SSH protocol encrypts all Internet traffic including passwords to eliminate eavesdropping, connection hijacking, and other network level attacks.

Operations Center

The home page of the Hercules Administrator console where you can monitor dashboard alerts, device discovery, device actions, compliance progress, remediation progress, V-Flash operations, and server maintenance.

Open Vulnerability Assessment Language (OVAL™)

An international, information security community baseline standard for how to check for the presence of vulnerabilities and configuration issues on computer systems. OVAL standardizes the three main steps of the process: 1) collecting system characteristics and configuration information from systems for testing, 2) testing the systems for the presence of specific vulnerabilities, configuration issues, and/or patches, and 3) presenting the results of the tests. OVAL definitions can be used by end users or implemented in scanning tools.

patch remedy

A Citadel-provided remedy that installs patches acquired from third-party independent software vendors. Hercules patch remedies are tested for patch interdependencies, pre-installation requirements, and conflict resolution to ensure fast and accurate patch application.

policy

A collection of remedies that are applied to groups of devices that share a common set of criteria. When you use policies and devices to create a policy enforcement, policies are applied on a recurring schedule.

policy catalog

Contains over 25 policies, both Citadel-defined policies and industry-defined policies, including DISA Security Checklist for Windows, FISMA Policy Templates, GLBA Policy Templates, HIPPA Policy Templates, NSA Windows Security Guides, the SANS Top 10 policies, Sarbanes-Oxley Policy templates, and a spyware removal policy.

policy enforcement

The systematic application of policies or action packs to devices in a network or as a condition of entering a network. You can apply a group of remedies to a group of devices that match a specific criteria, then schedule and monitor the enforcement and review its history. You can also create policy enforcements using ActionPacks with or without policies and with or without additional devices.

QuickStart

A wizard-guided mode designed to acquaint new Hercules users with basic workflows that can be performed from the Hercules Administrator console.

remediation

The application of remedies to selected devices to repair detected vulnerabilities imported from a scan. You can schedule remediations, monitor their progress, and review remediation history.

remediation mode

Use of the Hercules software with the Remediation feature licensed, which lets you perform policy enforcement, ActionPack enforcement, and remediation. Remediation history is retained and rollback functionality is available.

remedy

A set of remedial actions applied to a device to repair a specific vulnerability, if it exists. If the vulnerability does not exist, the device is considered to be in compliance. You can create custom remedies or use a Citadel-provided remedy, but you can only modify user-defined remedies.

remedy action

The building block for Citadel-provided and user-defined remedies. Each remedy action consists of two closely coupled parts: a compliance part that determines whether or not the device is compliant and an action part that applies the corrective action if needed.

remedy catalog

A list of all available Citadel-provided remedies and all user-defined remedies.

risk assessment

The feature included with AssetGuard that provides a way to assess a device's vulnerability risk and assign it a risk rating. The Risk rating is calculated based on the rating of the device's vulnerabilities, the sum of the technical assets running on the device (detected during inventory), and the user-defined business impact rating.

role-based security

Controls the Hercules tasks that users can perform based on their assigned role.

rollback

The ability to undo the changes to your Hercules system made during a remediation, when the changes produce unexpected an undesirable results. For rollback to function, a successful snapshot must have been taken prior to the remediation and the rollback must be invoked without interim system activity.

RSA algorithm

An encryption algorithm and authentication standard developed by Ron **Rivest**, Adi **Shamir**, and Leonard **Adleman.** RSA uses public-key cryptography that requires both a public key and a private key for message encryption/decryption. The RSA algorithm is the defacto standard for industrial-strength encryption especially for data sent over the Internet. It is built into many software products including the more popular web browsers such as Microsoft Internet Explorer.

scan

The process of assessing vulnerabilities on network devices using a third-party scanner. Each vulnerability detected is associated with the device containing the discovered vulnerability. When you import a scan into the Hercules database, you import detected vulnerabilities and data from the scanned devices.

Security Posture Display

A dashboard displaying network devices and groups on a graphical map that you can filter to help you identify security risks. You can display your network as a hierarchical, circular, or symmetrical map to assess network vulnerabilities and risks.

Secure Socket Shell (SSH)

A Unix-based command interface and protocol used to ensure secure communications with a remote computer. The protocol is widely used by network administrators to control Web and other kinds of servers remotely. SSH commands are encrypted and secure at both ends of the client/server connection by using encrypted digital certificates and passwords. SSH uses RSA public-key cryptography for both connection and authentication.

V-Flash server

The Citadel-provided server from which you can download the latest remedies, vulnerabilities, policies, and ActionPacks. Hercules software updates are also distributed via the V-Flash server.

vulnerability

A weakness that makes your device hardware or software vulnerable to virus attacks or unwanted intrusion. You can define custom vulnerabilities or use Citadel-provided vulnerabilities, but you can only modify user-defined vulnerabilities.

vulnerability catalog

A catalog of vulnerabilities, some of which are components of different policies. You can browse through details on vulnerabilities and their associated remedies, including remedy actions and properties.